This paper was published in *Semigroup Forum* **77** (2008), 36-63. To the best of my knowledge, this is the final version as it was submitted to the publisher. – NH

Digital Representation of Semigroups and Groups

Stefano Ferri[1]

Neil Hindman[2]

and

Dona Strauss

Abstract. A *digital representation* of a semigroup $(S, \cdot)$ is a family $\langle F_t \rangle_{t \in I}$, where I is a linearly ordered set, each F_t is a finite non-empty subset of S and every element of S is uniquely representable in the form $\Pi_{t \in H} x_t$ where H is a finite subset of I, each $x_t \in F_t$ and products are taken in increasing order of indices. (If S has an identity 1, then $\Pi_{t \in \emptyset} x_t = 1$.) A *strong digital representation* of a group G is a digital representation of G with the additional property that for each $t \in I$, $F_t = \{x_t, x_t^2, \ldots, x_t^{m_t - 1}\}$ for some $x_t \in G$ and some $m_t > 1$ in $\mathbb{N}$ where $m_t = 2$ if the order of x_t is infinite, while, if the order of x_t is finite, then m_t is a prime and the order of x_t is a power of m_t. We show that any free semigroup has a digital representation with each $|F_t| = 1$ and that each abelian group has a strong digital representation. We investigate the problem of whether all groups, or even all finite groups have strong digital representations, obtaining several partial results. Finally, we give applications to the algebra of the Stone-Čech compactification of a discrete group and the weakly almost periodic compactification of a discrete semigroup.

1. Introduction

There are many examples where one utilizes the ability to represent each element of an abelian group or semigroup $(S, +)$ in a unique fashion as $\sum_{t \in A} a_t x_t$ for $a_t \in D_t$ where $\langle x_t \rangle_{t \in A}$ is a given indexed set and D_t is a finite subset of $\mathbb{Z}$. The use of various fixed bases for the expansion of members of $\mathbb{N}$ as well as more esoteric variable bases are too numerous to cite here. Not so well known is the fact that with $x_t = (-2)^t$, $D_t = \{0, 1\}$, and $A = \omega = \mathbb{N} \cup \{0\}$, every element of $\mathbb{Z}$ has a unique expansion of the form $\sum_{t \in A} a_t x_t$ with each $a_t \in D_t$. This fact was used by B. Bordbar and J. Pym in [1] to show that there are $2^{\mathfrak{c}}$ idempotents in the weakly almost periodic compactification of $\mathbb{Z}$ and that the set of such idempotents is not closed. (A similar construction, wherein the coefficients rather than the base elements were allowed to be negative, was used also by W. A. F. Ruppert in [14] to produce weakly almost periodic functions.) In collaboration with

[1] This author was partially supported by a research grant of the Faculty of Sciences of *Universidad de los Andes*. The support is gratefully acknowledged.

[2] This author acknowledges support received from the National Science Foundation via Grant DMS-0554803.

I. Leader, we used a similar expansion to the base $-k$ in [7] to establish that certain natural infinite matrices are not image partition regular. A weak version of digital representation, the notion of *oid*, was introduced by J. Pym in [13] and is sufficient to derive much of the algebraic structure of the Stone-Čech compactification of $\mathbb{N}$.

Considerably more surprising was the fact that members of $\mathbb{Q}$ can be expressed uniquely in the form $\sum_{t\in A} a_t x_t$ for $a_t \in D_t$ where $A = \mathbb{Z}$, $x_t = \dfrac{(-1)^t}{(1-t)!}$ and $D_t = \{0, 1, \ldots, -t\}$ if $t < 0$, and $x_t = (-1)^t(1+t)!$ and $D_t = \{0, 1, \ldots, t+1\}$ if $t \geq 0$. T. Budak, N. Işik, and J. Pym established this fact in [2]. They used it to show that $\beta\mathbb{Q}_d$, the Stone-Čech compactification of $\mathbb{Q}$ with the discrete topology, has $2^{\mathfrak{c}}$ minimal left ideals and $2^{\mathfrak{c}}$ minimal right ideals, and each maximal group in its smallest ideal contains a free group on $2^{\mathfrak{c}}$ generators.

In [10] we investigated which semigroups have the property that there is some indexed family $\langle x_t\rangle_{t\in A}$ such that every element of the semigroup is uniquely representable in the form $\sum_{t\in F} x_t$. In the terms of the current paper, in which we are writing arbitrary semigroups multiplicatively, we were investigating which semigroups have digital representations $\langle F_t\rangle_{t\in I}$ with each $|F_t| = 1$.

In this paper we investigate more generally which semigroups have digital representations with specified properties. In Section 2 we show that any free semigroup has a digitial representation $\langle F_t\rangle_{t\in I}$ with each $|F_t| = 1$.

In Section 3 we turn our attention to groups. We show that any abelian group has a strong digital representation. We also show that if G is a group, H is a torsion group which is a normal subgroup of G and both H and G/H have strong digital representations, then so does G. As a consequence, if we knew that each finite simple group has a strong digital representation, we would know that the same statement would hold for any finite group. We succeed only in showing that the two classes of nonabelian finite simple groups which have the smallest members do all have strong digital representations.

In Section 4 we provide applications of our results to the algebra of the Stone-Čech compactification and the weakly almost periodic compactification of a discrete semigroup. Specifically we show that if a discrete semigroup T can be mapped homomorphically onto an infinite commutative cancellative semigroup of cardinality κ which has a digital representation, then the maximal groups in the smallest ideal of βT contain copies of the free group on 2^{2^κ} generators. We also show that, if T is an infinite discrete commutative group of cardinality κ, then the weakly almost periodic compactification

of T contains copies of the free abelian group on 2^{2^κ} generators.

We conclude the introduction with a general result applying to both semigroups and groups. Recall that the notions of *digital representation* and *strong digital representation* were defined in the abstract.

1.1 Lemma. *Let J be a set and for each $j \in J$, let S_j be a semigroup with identity 1 which has a digital representation. Then $S = \bigoplus_{j\in J} S_j$ has a digital representation. If each S_j is a group which has a strong digital representation, then S has a strong digital representation.*

Proof. For each $j \in J$ choose a digital representation $\langle F_{j,t}\rangle_{t\in I_j}$ of S_j, and choose a linear ordering of J. Let $I = \{(k,t) : k \in J \text{ and } t \in I_k\}$ and order I by agreeing that $(k,t) < (j,s)$ if either $k = j$ and $t < s$ or $k < j$. For each $k \in J$, let $\theta_k : S_k \to S$ denote the natural injection. It is routine to verify that $\langle \theta_k[F_{k,t}]\rangle_{(k,t)\in I}$ is a digital representation of S and, if each S_j is a group and $\langle F_{j,t}\rangle_{t\in I_j}$ is a strong digital representation of S_j, then $\langle \theta_k[F_{k,t}]\rangle_{(k,t)\in I}$ is a strong digital representation of S. □

2. Free semigroups

We show that all free semigroups have digital representations $\langle F_t\rangle_{t\in I}$ with each $|F_t| = 1$. We show also that if κ is the cardinality of the semigroup, then I can be chosen equal to κ with its ordering as an ordinal. (We are using the standard interpretation that κ is the first ordinal of its size. In particular the statements $\sigma < \kappa$ and $\sigma \in \kappa$ are synonymous.)

Given a set X we write $\mathcal{P}_f(X)$ for the set of finite nonempty subsets of X. Given $\langle x_t\rangle_{t\in I}$ where I is a linearly ordered set, we let

$$FP(\langle x_t\rangle_{t\in I}) = \{\textstyle\prod_{t\in F} x_t : F \in \mathcal{P}_f(I)\}$$

where the products are taken in increasing order of indices.

Notice that if S is the free semigroup (without identity) on an alphabet B and $\langle F_t\rangle_{t\in I}$ is a digital representation of S, then $\langle F_t\rangle_{t\in I}$ is also a digital representation of the free semigroup with identity on B. For $w \in S$ we write $\ell(w)$ for the length of the word w.

2.1 Lemma. *Let $\lambda > 0$ be a cardinal and let B be an alphabet with $|B| = \lambda$. Let S be the free semigroup on the alphabet B and let $\kappa = |S|$. For $w \in S$, let $A(w) = \{m \in S : m$ occurs in $w\}$. There is a well ordering $<$ of S in order type κ so that if $w, v \in S$, $A(w) \subseteq A(v)$, and $\ell(w) < \ell(v)$, then $w < v$.*

Proof. Notice that $\kappa = \max\{\lambda, \omega\}$. Well order B as $\langle a_\iota \rangle_{\iota<\lambda}$. For each $s \in S$, we define $f(s) < \lambda$ by $f(s) = \max(\{\iota < \lambda : a_\iota \text{ occurs in } s\})$. We put $g(s) = \max\{\ell(s), f(s)\}$. For each $\iota < \kappa$, we put $J_\iota = g^{-1}[\{\iota\}]$.

We make the following observations. The family $\{J_\iota : \iota < \kappa\}$ partitions S into disjoint subsets, J_ι is finite if ι is finite, and $|J_\iota| = |\iota|$ if ι is infinite.

We well order each J_ι in such a way that, for every $s, t \in J_\iota$, if $\ell(s) < \ell(t)$, then $s < t$. We then order S lexicographically by stating that $s < t$ if $g(s) < g(t)$ or if $g(s) = g(t)$ and $s < t$ in $J_{g(s)}$. This defines a well ordering of S of order type κ because, for every $\mu < \kappa$, $|\bigcup_{\iota<\mu} J_\iota| < \kappa$.

Now assume that $w, v \in S$, $A(w) \subseteq A(v)$, and $\ell(w) < \ell(v)$. Since $A(w) \subseteq A(v)$ we must have $f(w) \leq f(v)$. Therefore $g(w) \leq g(v)$. If $g(w) = g(v)$, then $w < v$ in $J_{g(w)}$ and consequently $w < v$. □

2.2 Theorem. *Let B be an alphabet, let S be the free semigroup on the alphabet B, and let $\kappa = |S|$. Then S has a digital representation $\langle F_\sigma \rangle_{\sigma<\kappa}$ with each $|F_\sigma| = 1$.*

Proof. For $w \in S$ let $A(w) = \{m \in S : m \text{ occurs in } w\}$. By Lemma 2.1 well order S in order type κ so that if $w, v \in S$, $A(w) \subseteq A(v)$, and $\ell(w) < \ell(v)$, then $w < v$.

Let $x_0 = \min S$. Let $\sigma < \kappa$ and assume we have chosen x_τ for $\tau < \sigma$. Then $|FP(\langle x_\tau \rangle_{\tau<\sigma})| < \kappa$ so $S \setminus FP(\langle x_\tau \rangle_{\tau<\sigma}) \neq \emptyset$. Let $x_\sigma = \min\big(S \setminus FP(\langle x_\tau \rangle_{\tau<\sigma})\big)$.

Since the ordering of S is in order type κ we have that $S = FP(\langle x_\sigma \rangle_{\sigma<\kappa})$. Note also that

$(*)$ if $w \in S$, $\sigma < \kappa$, $A(w) \subseteq A(x_\sigma)$, and $\ell(w) < \ell(x_\sigma)$, then $w \in FP(\langle x_\tau \rangle_{\tau<\sigma})$.

Suppose we have $F \neq G$ in $\mathcal{P}_f(\kappa)$ such that $\prod_{\sigma\in F} x_\sigma = \prod_{\sigma\in F} x_\sigma$. By right cancellation we may assume that $\tau = \max F \neq \max G = \delta$. Further, if we had $\ell(x_\tau) = \ell(x_\delta)$ we would have $x_\tau = x_\delta$, so we may assume that $\ell(x_\tau) > \ell(x_\delta)$. And then, since $A(x_\delta) \subseteq A(x_\tau)$ we have by $(*)$ that $x_\delta \in FP(\langle x_\eta \rangle_{\eta<\tau})$ and so $\delta < \tau$.

For $\sigma \in G$, let $H_\sigma = \{\mu \in G : \sigma \leq \mu\}$. Let $\eta = \min\{\sigma \in G : \ell(\prod_{\mu\in H_\sigma} x_\mu) \leq \ell(x_\tau)\}$. We cannot have $\ell(\prod_{\mu\in H_\eta} x_\mu) = \ell(x_\tau)$ for then we would have $x_\tau = \prod_{\mu\in H_\eta} x_\mu \in FP(\langle x_\mu \rangle_{\mu\leq\delta}) \subseteq FP(\langle x_\mu \rangle_{\mu<\tau})$. So $\ell(\prod_{\mu\in H_\eta} x_\mu) < \ell(x_\tau)$. So there exist letters $m_1, m_2, \ldots, m_s$ such that $x_k = m_1 \cdot m_2 \cdots m_s \prod_{\mu\in H_\eta} x_\mu$. Let $\gamma = \max(G \setminus H_\eta)$. Then $\gamma < \eta$ so

$$\begin{aligned} \ell(x_\gamma) + \ell(\textstyle\prod_{\mu\in H_\eta} x_\mu) &= \ell(\textstyle\prod_{\mu\in H_\gamma} x_\mu) \\ &> \ell(x_\tau) \\ &= s + \ell(\textstyle\prod_{\mu\in H_\eta} x_\mu) \end{aligned}$$

so $s < \ell(x_\gamma)$ and by $(*)$ $m_1 \cdot m_2 \cdots m_s \in FP(\langle x_\mu \rangle_{\mu<\gamma}) \subseteq FP(\langle x_\mu \rangle_{\mu<\eta})$ so $x_\tau \in FP(\langle x_\mu \rangle_{\mu\leq\delta}) \subseteq FP(\langle x_\mu \rangle_{\mu<\tau})$, a contradiction.

The induction being complete, let $F_\sigma = \{x_\sigma\}$ for each $\sigma < \kappa$. □

3. Groups

Now we turn our attention to groups. In this section we will write "$(\langle x_t \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$ *is a digital representation of* S" to represent the statement that $\langle F_t \rangle_{t\in I}$ is a digital representation of S and for each $t \in I$, $F_t = \{x_t, x_t^2, \ldots, x_t^{m_t-1}\}$. Then the assertion "$(\langle x_t \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$ *is a strong digital representation of* S" adds the requirement that $m_t = 2$ when x_t has infinite order and if the order of x_t is finite then that order is the power of a prime p and $m_t = p$.

3.1 Lemma. *Let H and K be subgroups of a group G such that $H \cap K = \{1\}$ and HK is a group. Assume that $(\langle x_t \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$ is a digital representation of H and $(\langle y_t \rangle_{t\in J}, \langle n_t \rangle_{t\in J})$ is a digital representation of K. Let $L = (I \times \{1\}) \cup (J \times \{2\})$ and order L by agreeing that $I \times \{1\}$ precedes $J \times \{2\}$ (and of course internal order is preserved). For $t \in I$, let $z_{(t,1)} = x_t$ and $r_{(t,1)} = m_t$, and for $t \in J$, let $z_{(t,2)} = y_t$ and $r_{(t,2)} = n_t$. Then $(\langle z_{(t,i)} \rangle_{(t,i)\in L}, \langle r_{(t,i)} \rangle_{(t,i)\in L})$ is a digital representation of HK. In particular, if H and K have strong digital representations, so does HK.*

Proof. Trivially each element of HK is representable in the form

$$\left(\prod_{t\in F} (x_t)^{\alpha(t)}\right)\left(\prod_{t\in P} (y_t)^{\delta(t)}\right)$$

for some finite (possibly empty) subsets F of I and P of J and some choice of $\alpha(t) \in \{1, 2, \ldots, m_t - 1\}$ for $t \in F$ and some choice of $\delta(t) \in \{1, 2, \ldots, n_t - 1\}$ for $t \in P$. Suppose that we have finite subsets F and F' of I and P and P' of J and choices of $\alpha(t)$ for $t \in F$, $\alpha'(t)$ for $t \in F'$, $\delta(t)$ for $t \in P$, and $\delta'(t)$ for $t \in P'$ such that $\left(\prod_{t\in F} (x_t)^{\alpha(t)}\right)\left(\prod_{t\in P} (y_t)^{\delta(t)}\right) = \left(\prod_{t\in F'} (x_t)^{\alpha'(t)}\right)\left(\prod_{t\in P'} (y_t)^{\delta'(t)}\right)$. Then $\left(\prod_{t\in F'} (x_t)^{\alpha'(t)}\right)^{-1}\left(\prod_{t\in F} (x_t)^{\alpha(t)}\right) = \left(\prod_{t\in P'} (y_t)^{\delta'(t)}\right)\left(\prod_{t\in P} (y_t)^{\delta(t)}\right)^{-1} \in H \cap K = \{1\}$ so $(F, \alpha) = (F', \alpha')$ and $(P, \delta) = (P', \delta')$. □

3.2 Lemma. *Let H be a normal subgroup of a group G. Assume that G/H has a digital representation $(\langle x_t H \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$, $(\langle y_t \rangle_{t\in J}, \langle n_t \rangle_{t\in J})$ is a digital representation of H, and $I \cap J = \emptyset$. Let $L = I \cup J$ and order L by agreeing that I preceeds J. For $t \in I$, let $z_t = x_t$ and $r_t = m_t$, and for $t \in J$, let $z_t = y_t$ and $r_t = n_t$. Then $(\langle z_t \rangle_{t\in L}, \langle r_t \rangle_{t\in L})$ is a digital representation of G.*

Proof. We first show that each $w \in G$ is representable in the form

$$\left(\prod_{t\in F}(x_t)^{\alpha(t)}\right)\left(\prod_{t\in P}(y_t)^{\delta(t)}\right)$$

for some finite (possibly empty) subsets F of I and P of J and some choice of $\alpha(t) \in \{1, 2, \ldots, m_t - 1\}$ for $t \in F$ and some choice of $\delta(t) \in \{1, 2, \ldots, n_t - 1\}$ for $t \in P$. If $w \in H$, this is trivial, so assume that $w \in G \setminus H$. Pick finite $F \subseteq I$ and a choice of $\alpha(t) \in \{1, 2, \ldots, m_t - 1\}$ for $t \in F$ such that $wH = \prod_{t\in F}(x_t H)^{\alpha(t)}$. Then $w \in \left(\prod_{t\in F}(x_t)^{\alpha(t)}\right)H$ so pick $z \in H$ such that $w = \left(\prod_{t\in F}(x_t)^{\alpha(t)}\right)z$. Pick finite $P \subseteq J$ and a choice of $\delta(t) \in \{1, 2, \ldots, n_t - 1\}$ for $t \in P$ such that $z = \prod_{t\in P}(y_t)^{\delta(t)}$.

Now suppose that we have finite subsets F and F' of I and P and P' of J and choices of $\alpha(t)$ for $t \in F$, $\alpha'(t)$ for $t \in F'$ $\delta(t)$ for $t \in P$, and $\delta'(t)$ for $t \in P'$ such that $\left(\prod_{t\in F}(x_t)^{\alpha(t)}\right)\left(\prod_{t\in P}(y_t)^{\delta(t)}\right) = \left(\prod_{t\in F'}(x_t)^{\alpha'(t)}\right)\left(\prod_{t\in P'}(y_t)^{\delta'(t)}\right)$. Then $\left(\prod_{t\in F'}(x_t)^{\alpha'(t)}\right)^{-1}\left(\prod_{t\in F}(x_t)^{\alpha(t)}\right) = \left(\prod_{t\in P'}(y_t)^{\delta'(t)}\right)\left(\prod_{t\in P}(y_t)^{\delta(t)}\right)^{-1} \in H$ so $\left(\prod_{t\in F'}(x_t)^{\alpha'(t)}\right)H = \left(\prod_{t\in F}(x_t)^{\alpha(t)}\right)H$ so $\prod_{t\in F'}(x_t H)^{\alpha'(t)} = \prod_{t\in F}(x_t H)^{\alpha(t)}$. So $(F, \alpha) = (F', \alpha')$ and therefore $\prod_{t\in P}(y_t)^{\delta(t)} = \prod_{t\in P'}(y_t)^{\delta'(t)}$ and thus $(P, \delta) = (P', \delta')$. □

Recall that a *torsion* group is one in which each element has finite order and a *torsion free* group is one in which no element has finite order. In what follows, given a group G and an element $g \in G$, we shall denote by $o(g)$ the order of g.

3.3 Lemma. *Let G be a group and let H be a torsion group which is a normal subgroup of G. Let p be a prime, let $k \in \mathbb{N}$, and assume that $y \in G$ is such that $o(yH) = p^k$. Then there exist $x \in G$ and $n \in \mathbb{N}$ such that $xH = yH$ and $o(x) = p^n$.*

Proof. Since $y^{p^k} \in H$, y has finite order. Let $m = o(y)$. If $m = p^k$, we are done, so assume $m > p^k$. Now $y^m = 1 \in H$ so $(yH)^m = H$ so p^k divides m. Pick $t \geq k$ and q relatively prime to p such that $m = qp^t$. Pick by the Chinese Remainder Theorem some $z \in \mathbb{N}$ such that $z \equiv 0 \pmod{q}$ and $z \equiv 1 \pmod{p^k}$. Pick $r, s \in \omega$ such that $z = rq = sp^k + 1$. Let $x = y^z$. Then $xH = y^{sp^k+1}H = (yH)^{p^k s}yH = yH$. Also $x^{p^t} = y^{rqp^t} = (y^m)^r = 1$ so $o(x)$ divides p^t. □

Note that one cannot omit the assumption that H is a torsion group in either the above lemma or the following theorem. To see this let $G = (\mathbb{Z}, +)$ and let $H = 3\mathbb{Z}$. Then $o(1 + H) = 3$ but no $x \in G$ has finite order. Further, no strong digital representation of H extends to a strong digital representation of G.

3.4 Theorem. *Let G be a group, let H be a torsion group which is a normal subgroup of G, and assume that H and G/H have strong digital representations. Then so does G. In fact, if $(\langle y_t\rangle_{t\in J}, \langle n_t\rangle_{t\in J})$ is a strong digital representation of H, then there exist L containing J and a strong digital representation $(\langle z_t\rangle_{t\in L}, \langle r_t\rangle_{t\in L})$ of G such that t precedes s whenever $t \in L \setminus J$ and $s \in J$ and $z_t = y_t$ and $r_t = n_t$ whenever $t \in J$.*

Proof. Lemmas 3.2 and 3.3. □

3.5 Corollary. *If each finite simple group has a strong digital representation, then every finite group has a strong digital representation.*

Proof. Induction on $|G|$ using Theorem 3.4. □

We now set out to show in Theorem 3.9 that every abelian group has a strong digital representation.

3.6 Lemma. *Let G be an abelian torsion group, let P be the set of primes, and for $p \in P$, let $A_p = \{x \in G : o(x) = p^k \text{ for some } k \in \omega\}$. Then each A_p is a subgroup of G and $G \cong \bigoplus_{p\in P} A_p$.*

Proof. [6, Theorem A3]. □

3.7 Lemma. *Let p be a prime and let G be an abelian group such that $o(x)$ is a power of p for each $x \in G$. Then G has a strong digital representation.*

Proof. For each $n \in \mathbb{N}$, let $G_n = \{a \in G : a^{p^n} = 1\}$. Then each G_n is a subgroup of G. We produce inductively a possibly empty set A_n and $\langle x_t\rangle_{t\in A_n}$ such that $A_n \cap A_k = \emptyset$ for $n \neq k$ and if $B_m = \bigcup_{n=1}^m A_n$ and for each $t \in B_m$, $r_t = p$, then for each $m \in \mathbb{N}$, $(\langle x_t\rangle_{t\in B_m}, \langle r_t\rangle_{t\in B_m})$ is a strong digital representation of G_m.

We have that G_1 is a vector space over $\mathbb{Z}_p$, so is isomorphic to a direct sum of copies of $\mathbb{Z}_p$ hence, by Lemma 1.1, G_1 has a strong digital representation.

Pick A_1 and $\langle x_t\rangle_{t\in A_1}$ such that $(\langle x_t\rangle_{t\in A_1}, \langle r_t\rangle_{t\in A_1})$ is a strong digital representation of G_1 where $r_t = p$ for each $t \in A_1$.

Inductively, let $m \in \mathbb{N}$ and assume that A_n and $\langle x_t\rangle_{t\in A_n}$ have been chosen for $n \leq m$. Now given $w \in G_{m+1}$, $w^p \in G_m$ so G_{m+1}/G_m is a vector space over $\mathbb{Z}_p$ and therefore has a strong digital representation.

By Theorem 3.4 we may choose a set A_{m+1} disjoint from $B_m = \bigcup_{n=1}^m A_n$ and $\langle x_t\rangle_{t\in A_{m+1}}$ such that $(\langle x_t\rangle_{t\in B_m\cup A_{m+1}}, \langle r_t\rangle_{t\in B_m\cup A_{m+1}})$ is a strong digital representation of G_{m+1} where each $r_t = p$.

The induction being complete, let $B = \bigcup_{n=1}^{\infty} A_n$. Then $(\langle x_t \rangle_{t\in B}, \langle r_t \rangle_{t\in B})$ is a strong digital representation of G. □

3.8 Lemma. *Let G be an abelian torsion free group. Then G has a strong digital representation.*

Proof. [10, Theorem 4.7]. □

3.9 Theorem. *Every abelian group has a strong digital representation.*

Proof. Let G be an abelian group, let $T = \{x \in G : o(x) \text{ is finite}\}$. Let P be the set of primes, and for $p \in P$, let $A_p = \{x \in T : o(x) = p^k \text{ for some } k \in \omega\}$. By Lemma 3.6, $T \cong \bigoplus_{p\in P} A_p$ so by Lemmas 3.7 and 1.1, T has a strong digital representation.

Now G/T is torsion free so by Lemma 3.8, G/T has a strong digital representation. By Theorem 3.4, G has a strong digital representation. □

3.10 Lemma. *Every finite nonabelian simple group has an order which has a repeated prime factor.*

Proof. In [5, Table 1] the orders of the finite simple groups are listed. A simple check shows that each has a repeated prime factor. □

Notice that the requirement in the following theorem regarding no repeated prime factors cannot simply be omitted. Indeed, $\mathbb{Z}_4$ does not have a digital representation with each x_t having order 2.

3.11 Theorem. *Let G be a finite group and assume that $|G|$ is a product of distinct primes. Then G has a strong digital representation $(\langle x_t \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$ with the additional property that each x_t has order m_t.*

Proof. We proceed by induction on the length of the prime factorization of $|G|$. If $|G|$ is a prime p, then G is isomorphic to $\mathbb{Z}_p$ which has a digital representation of the required type. Assume now that $|G|$ is a product of more than 1 distinct primes and the result is valid for groups with shorter factorizations of their order. By Lemma 3.10 G is not simple so pick a proper normal subgroup H of G. Then H and G/H each have a digital representation of the required type. Assume that $(\langle x_t H \rangle_{t\in I}, \langle m_t \rangle_{t\in I})$ is a digital representation of G/H where each $m_t = o(x_t)$ and m_t is a prime. By Lemma 3.3 one may choose for each $t \in I$ some $z_t \in G$ such that $z_t H = x_t H$ and $o(z_t) = (m_t)^n$ for some $n \in \mathbb{N}$. But since $|G|$ has no repeated prime factors, we know that $n = 1$. The result now follows from Lemma 3.2. □

3.12 Theorem. *If G is a group such that $|G|$ has at most 2 distinct prime factors, then G has a strong digital representation.*

Proof. Assume first that $|G| = p^k$ for some prime p and some $k \in \mathbb{N}$. By Lemma 3.7 G has a strong digital representation.

Now, assume $|G| = p^k q^l$ where p and q are primes. Pick by Sylow's Theorem subgroups H and K with $|H| = p^k$ and $|K| = q^l$. Then $H \cap K = \{1\}$ so Lemma 3.1 applies. □

We now set out to show in Theorem 3.18 that any group of order p^2qr has a strong digital representation. Actually, a considerably stronger result holds. We have by Theorems 3.20 and 3.29 below that all of the groups A_n and $A_n(q)$ where $n \in \mathbb{N}$ and q is a power of a prime have strong digital representations. According to [5, Table 1] any nonabelian simple group which is not of this form has an order whose prime factorization has length at least 8. Consequently, by Theorem 3.4 any finite group whose order has a prime factorization of length less than 8 must have a strong digital representation. However, we do feel that there is some virtue in a result whose proof does not rely on the classification of the finite simple groups.

3.13 Lemma. *Let p, q, and r be primes and let G be a group with $|G| = p^2qr$. If G has a subgroup H with size pqr, qr, p^2q, or p^2r, then G has a strong digital representation.*

Proof. Assume first that $|H| \in \{qr, p^2q, p^2r\}$. By Theorem 3.12 H has a strong digital representation. Pick a subgroup K such that $|K|$ is respectively p^2, r, or q. Then K has a strong digital representation so Lemma 3.1 applies.

Now assume that $|H| = pqr$. By Theorem 3.11, H has a strong digital representation. Pick a subgroup M of G with $|M| = p^2$. Pick $x \in M \setminus H$. Then $\{x, x^2, \ldots, x^{p-1}\} \cap H = \emptyset$. (Suppose $t \in \{1, 2, \ldots, p-1\}$ and $x^t \in H$. Pick by the Chinese Remainder Theorem $k \in \mathbb{N}$ such that $k \equiv 0 \pmod{t}$ and $k \equiv 1 \pmod{o(x)}$. Then $x = x^k \in H$.) We claim that every member of G is uniquely representable in the form zx^t for $z \in H$ and $t \in \{0, 1, \ldots, p-1\}$. Since $|G| = |H| \cdot p$ it suffices to establish uniqueness. Suppose $z, w \in H$ and $t, s \in \{0, 1, \ldots, p-1\}$ with $t \leq s$ and $zx^t = wx_s$. Then $x^{s-t} = w^{-1}z \in H$, so $s = t$ so $z = w$. □

3.14 Lemma. *Let G be a group, let H be a subgroup of G, and let $N_H = \{x \in G : xH = Hx\}$. If $N_H = H$, $x, y \in G$, and $xH \neq yH$, then $xHx^{-1} \neq yHy^{-1}$.*

Proof. If $xHx^{-1} = yHy^{-1}$, then $y^{-1}xH = Hy^{-1}x$ so $y^{-1}x \in N_H = H$ so $xH = yH$. □

3.15 Lemma. *Let p, q, and r be primes and let G be a group with $|G| = p^2qr$. If G does not have a strong digital representation, then G has at least $(q-1)pr$ elements of order q and at least $(r-1)pq$ elements of order r.*

Proof. It suffices to show that there are at least $(q-1)pr$ elements of order q. Pick a subgroup H of G with $|H| = q$. Let $N_H = \{x \in G : xH = Hx\}$. Then $H \subseteq N_H$ and N_H is a group, so $|N_H| \in \{q, pq, qr, pqr, p^2q, p^2qr\}$. By Lemma 3.13, $|N_H| \notin \{qr, pqr, p^2q\}$.

Suppose $|N_H| = p^2qr$. That is, $N_H = G$. Then H is a normal subgroup of G. Since $|H| = q$ and $|G/H| = p^2r$ we have by Theorem 3.12 that H and G/H have strong digital representations hence, by Theorem 3.4, so does G, a contradiction.

Thus $|N_H| = q$ or $|N_H| = pq$. Assume first that $|N_H| = q$ so that $N_H = H$. By Lemma 3.14, if $xH \neq yH$, then $xHx^{-1} \neq yHy^{-1}$. There are p^2r left cosets of H and if $xHx^{-1} \neq yHy^{-1}$, then $xHx^{-1} \cap yHy^{-1} = \{1\}$, so $|\bigcup_{x\in G} xHx^{-1}| = p^2r(q-1)+1$ so there are at least $p^2r(q-1)$ elements of order q.

Now assume that $|N_H| = pq$. We claim that if $y \in N_H$ and $o(y) = q$, then $y \in H$. Indeed, pick $x \in N_H$ such that $o(x) = p$ and pick $a \in H \setminus \{1\}$. Then $\{x^t a^s : t \in \{0, 1, \ldots, p-1\}$ and $s \in \{0, 1, \ldots, q-1\}\}$ is a subset of N_H with pq elements, so it equals N_H. Note that if $t \in \{1, 2, \ldots, p-1\}$ and $s \in \{0, 1, \ldots, q-1\}$, then $o(x^t a^s)$ is either p or pq. (We have that $x^t \in N_H$ so $(x^tH)^q = x^{tq}H$ so $(x^ta^s)^q = x^{tq}b$ for some $b \in H$. Since $b \in H$ and $x^{tq} \neq 1$, $x^{tq}b \neq 1$.) Thus the only elements of N_H of order q must be of the form x^0a^s, as required.

Next we claim that if $H \cap uN_Hu^{-1} \neq \{1\}$, then $H = uHu^{-1}$. Note that $H \cap uN_Hu^{-1}$ is a nontrivial subgroup of H, so $H = H \cap uN_Hu^{-1}$. That is $H \subseteq uN_Hu^{-1}$. To see that $H \subseteq uHu^{-1}$, let $y \in H$. If $y = 1$, then $y \in uHu^{-1}$ so assume that $y \neq 1$. Then $u^{-1}yu \in N_H$ and $o(u^{-1}yu) = q$ so $u^{-1}yu \in H$. Thus $y \in uHu^{-1}$. Since $H \subseteq uHu^{-1}$ and $|H| = |uHu^{-1}|$ we have $H = uHu^{-1}$.

Now we claim that if $uN_H \neq vN_H$, then $(uN_Hu^{-1}) \cap (vN_Hv^{-1})$ contains no elements of order q. Suppose instead we have $y \in (uN_Hu^{-1}) \cap (vN_Hv^{-1})$ with $o(y) = q$. Then $u^{-1}yu \in N_H \cap u^{-1}vN_Hv^{-1}u$. Since $o(u^{-1}yu) = q$ and $u^{-1}yu \in N_H$, we have $u^{-1}yu \in H$ so $H \cap u^{-1}vN_Hv^{-1}u \neq \{1\}$. Thus $H = u^{-1}vHv^{-1}u \neq \{1\}$, so $v^{-1}u \in N_H$ and therefore $uN_H = vN_H$, a contradiction.

Since there are pr left cosets of N_H and each uN_Hu^{-1} has $q-1$ elements of order q, there are at least $(q-1)pr$ elements of order q in G. □

3.16 Lemma. *Let p, q, and r be primes and let G be a group with $|G| = p^2qr$. Assume that $a \in G$ and $o(a) = p^2$. Let $H = \{1, a, a^2, \ldots, a^{p^2-1}\}$, let $N_a = \{x \in G : ax = xa\}$,*

and let $N_H = \{x \in G : xH = Hx\}$. *If* G *does not have a strong digital representation, then* $N_a = N_H = H$.

Proof. Trivially, $N_a = N_H$ and $H \subseteq N_H$. So p^2 divides $|N_H|$. It suffices to show that $|N_H| = p^2$. By Lemma 3.13 $|N_H| \neq p^2q$ and $|N_H| \neq p^2r$. Suppose that $|N_H| = p^2qr$. Pick subgroups K and M of G with $|K| = q$ and $|M| = r$. Then, by Theorem 3.12, H, K, and M have strong digital representations. Since $K \subseteq N_H$, by Lemma 3.1, HK is a group which has a strong digital representation. Then $|MHK| = p^2qr$ so, by Lemma 3.1, $G = MHK$ has a strong digital representation. □

3.17 Lemma. *Let* p, q, *and* r *be primes and let* G *be a group with* $|G| = p^2qr$. *Let* A *and* B *be distinct subgroups of* G *with* $|A| = |B| = p^2$. *If* G *does not have a strong digital representation, then* $A \cap B$ *is contained in the center of* G.

Proof. Suppose we have $a \in (A \cap B) \setminus Z(G)$. Since any group of order p^2 is abelian, $A \subseteq N_a$, so p^2 divides $|N_a|$. By Lemma 3.13 $|N_a| \neq p^2q$ and $|N_a| \neq p^2r$. If we had $|N_a| = p^2qr$, then we would have $N_a = G$ and so $a \in Z(G)$. Thus $|N_a| = p^2$. Since $A \cup B \subseteq N_a$, we have $|A \cup B| = p^2$ so $A = B$. □

3.18 Theorem. *Let* p, q, *and* r *be primes and let* G *be a group with* $|G| = p^2qr$. *Then* G *has a strong digital representation.*

Proof. Suppose not. Pick a subgroup H with $|H| = p^2$. Assume first that H has an element x with $o(x) = p^2$. Then for $t \in \{1, 2, \ldots, p^2 - 1\}$,

$$o(x^t) = \begin{cases} p & \text{if } t \in \{p, 2p, \ldots, (p-1)p\} \\ p^2 & \text{otherwise.} \end{cases}$$

So H has $p^2 - p$ elements of order p^2. None of these occur in another subgroup of order p^2 since the intersection of two distinct groups of order p^2 has either 1 or p elements. By Lemma 3.16 $N_H = H$ so, by Lemma 3.14, if $x, y \in G$ and $xH \neq yH$, we have $x^{-1}Hx \neq y^{-1}Hy$. Since H has qr cosets, there are at least $qr(p^2 - p)$ elements of order p^2. (We shall show later that there cannot be this many elements of order p^2.)

Assume now that H has no element of order p^2. We claim that H is not contained in the center of G. Suppose it is and pick subgroups K and M of order q and r respectively. Then H, K, and M have strong digital representations by Theorem 3.12. Since $H \subseteq Z(G)$, HK is a group which has a strong digital representation by Lemma 3.1. Then $|MHK| = p^2qr$ so $G = MHK$ has a strong digital representation by Lemma 3.1.

Thus $H \cap Z(G)$ is a proper subgroup of H so has at most p elements. Next we claim that $N_H = H$. Since $H \subseteq N_H$ we have that p^2 divides $|N_H|$. By Lemma 3.13, $|N_H|$ is neither of p^q or $p^2 r$. If $|N_H| = p^2 qr$, then as above pick subgroups K and M of order q and r respectively. Then H, K, and M have strong digital representations by Theorem 3.12. Since $K \subseteq N_H$, HK is a group which has a strong digital representation by Lemma 3.1. Then $|MHK| = p^2 qr$ so $G = MHK$ has a strong digital representation by Lemma 3.1. So $N_H = H$ as claimed.

By Lemma 3.17 if $xHx^{-1} \neq yHy^{-1}$, then $xHx^{-1} \cap yHy^{-1} \subseteq Z(G)$ so $xHx^{-1} \setminus Z(G)$ and $yHy^{-1} \setminus Z(G)$ are disjoint. By Lemma 3.14 if $xH \neq yH$, then $xHx^{-1} \neq yHy^{-1}$. So $|\bigcup_{x \in G} xHx^{-1}| \geq qr(p^2 - p) + p$.

Thus in any event there are at least $qr(p^2 - p)$ elements of order p or p^2. But also by Lemma 3.15 there are at least $(q-1)pr$ elements of order q and at least $(r-1)qp$ elements of order r. But $qr(p^2-p) + (q-1)pr + (r-1)qp = p^2 qr + p(qr - q - r) > p^2 qr$, a contradiction. □

Because of Corollary 3.5 we are interested in the finite simple groups, which would necessarily provide the smallest counterexamples to the assertion that each group, or at least each finite group, has a strong digital representation. The smallest non-abelian simple group is A_5, the alternating group on 5 elements. Further, A_n is simple for all $n \geq 5$. The same proof applies to the full symmetric group, so we give it as well.

In the following, $\prod_{t=n}^{1} x_t = x_n x_{n-1} \cdots x_1$.

3.19 Lemma. *Let $n \in \mathbb{N} \setminus \{1, 2\}$ and let $G = A_{n-1}$ and $K = A_n$ or let $G = S_{n-1}$ and $K = S_n$. Assume that $(\langle x_t \rangle_{t=1}^k, \langle m_t \rangle_{t=1}^k)$ is a digital representation of G. Let $\langle y_t \rangle_{t=1}^l$ be a sequence in $K \setminus G$ and let $\langle p_t \rangle_{t=1}^l$ be a sequence in $\mathbb{N} \setminus \{1\}$. Assume that $p_t = o(y_t)$ for each $t \in \{1, 2, \ldots, l\}$ and $(y_t)^a \notin G$ for each $t \in \{1, 2, \ldots, l\}$ and each $a \in \{1, 2, \ldots, p_t - 1\}$. For $t \in \{1, 2, \ldots, k + l\}$ define*

$$z_t = \begin{cases} x_t & \text{if } t \leq k \\ y_{t-k} & \text{if } t > k \end{cases} \text{ and } s_t = \begin{cases} m_t & \text{if } t \leq k \\ r_{t-k} & \text{if } t > k \end{cases}$$

Assume further that whenever $q \in \{2, 3, \ldots, l\}$, a_t and b_t are in $\{0, 1, \ldots, p_t - 1\}$, and $c \in \{1, 2, \ldots, p_q - 1\}$ one has that $\left(\prod_{t=1}^{q-1} (y_t)^{a_t}\right) (y_q)^c \left(\prod_{t=q-1}^{1} (y_t)^{b_t}\right) \notin G$. Then whenever a_t and b_t are in $\{0, 1, \ldots, s_t\}$ for each $t \in \{1, 2, \ldots, k + l\}$ and $\prod_{t=1}^{k+l} (z_t)^{a_t} = \prod_{t=1}^{k+l} (z_t)^{b_t}$, one must have $a_t = b_t$ for each $t \in \{1, 2, \ldots, k + l\}$.

Proof. Since $(\langle x_t \rangle_{t=1}^k, \langle m_t \rangle_{t=1}^k)$ is a digital representation of G, it suffices to show that if $u, v \in G$ and a_t and b_t are in $\{0, 1, \ldots, p_t - 1\}$ for each $t \in \{1, 2, \ldots, l\}$, if $u \prod_{t=1}^{l} (y_t)^{a_t} = v \prod_{t=1}^{l} (y_t)^{b_t}$, then $a_t = b_t$ for each t. Suppose instead that this fails

and pick the largest $q \in \{1, 2, \ldots, l\}$ such that $a_q \neq b_q$ and assume without loss of generality that $a_q > b_q$. If $q = 1$, then we have $(y_1)^{a_1 - b_1} = u^{-1}v \in G$, a contradiction. So assume that $q > 1$. Then $\left(\prod_{t=1}^{q-1}(y_t)^{a_t}\right)(y_q)^{a_q - b_q}\left(\prod_{t=q-1}^{1}(y_t)^{p_t - b_t}\right) = u^{-1}v \in G$, a contradiction. □

3.20 Theorem. *For each $n \in \mathbb{N} \setminus \{1, 2\}$, A_n and S_n have strong digital representations $(\langle x_t \rangle_{t \in I}, \langle m_t \rangle_{t \in I})$ with the additional property that each x_t has order m_t.*

Proof. We proceed by induction on n. If $n = 3$, the results are trivial.

Now let $n > 3$ and let $G = A_{n-1}$ and $K = A_n$ or let $G = S_{n-1}$ and $K = S_n$. Let $(\langle x_t \rangle_{t=1}^{k}, \langle m_t \rangle_{t=1}^{k})$ be a digital representation of G with the required property. Factor n as $p_1 p_2 \cdots p_l$ where each p_i is a prime and, if n is even, $p_1 = 2$. Since $|K| = |G| \cdot \prod_{t=1}^{l} p_t$, by Lemma 3.19, it suffices to produce $y_t \in K \setminus G$ for each $t \in \{1, 2, \ldots, l\}$ such that $(y_t)^a \notin G$ for each $t \in \{1, 2, \ldots, l\}$ and each $a \in \{1, 2, \ldots, p_t - 1\}$ and whenever $q \in \{2, 3, \ldots, l\}$, a_t and b_t are in $\{0, 1, \ldots, p_t - 1\}$, and $c \in \{1, 2, \ldots, p_q - 1\}$ one has that $\left(\prod_{t=1}^{q-1}(y_t)^{a_t}\right)(y_q)^c\left(\prod_{t=q-1}^{1}(y_t)^{b_t}\right) \notin G$.

If $p_1 = 2$, let $y_1 = (n-1, n)(1, 2)$ and let $B_1 = \{n-1, n\}$. Otherwise, let y_1 be a p_1-cycle including n and let B_1 be the set of terms of that cycle. Let $k \in \{1, 2, \ldots, l-1\}$ and assume that we have chosen y_k and B_k so that $|B_k| = \prod_{i=1}^{k} p_i$ and, unless $k = 1$ and $p_1 = 2$, B_k is the set of numbers moved by y_k. Let y_{k+1} consist of $|B_k|$ disjoint p_{k+1}-cycles, each of which includes exactly one term from B_k. Unless $k = l - 1$, make sure that neither 1 nor 2 is moved by p_{k+1}.

For example, if $n = 36 = 2 \cdot 3 \cdot 3 \cdot 2$, let

$$\begin{aligned}
y_1 =&(35, 36)(1, 2)\\
y_2 =&(31, 32, 35)(33, 34, 36)\\
y_3 =&(19, 20, 31)(21, 22, 32)(23, 24, 33)(25, 26, 34)(27, 28, 35)(29, 30, 36)\\
y_4 =&(1, 19)(2, 20)(3, 21)(4, 22)(5, 23)(6, 24)(7, 25)(8, 26)(9, 27)\\
&(10, 28)(11, 29)(12, 30)(13, 31)(14, 32)(15, 33)(16, 34)(17, 35)(18, 36)\,.
\end{aligned}$$

Now let $q \in \{2, 3, \ldots, l\}$ and choose a_t and b_t in $\{0, 1, \ldots, p_t - 1\}$ for each $t \in \{1, 2, \ldots, q-1\}$ and $c \in \{1, 2, \ldots, p_q - 1\}$ and let $w = \left(\prod_{t=1}^{q-1}(y_t)^{a_t}\right)(y_q)^c\left(\prod_{t=q-1}^{1}(y_t)^{b_t}\right)$. We need to show that $w \notin G$, that is, that w moves n. Let $m = \left(\prod_{t=q-1}^{1}(y_t)^{b_t}\right)(n)$. Then $m \in B_{q-1}$ and $c \neq 0$ so $(y_q)^c(m) \in B_q \setminus B_{q-1}$. Therefore

$$\left(\prod_{t=2}^{q-1}(y_t)^{a_t}\right)\left((y_q)^c(w)\right) = (y_q)^c(w)\,.$$

If $q = l$, then possibly $(y_q)^c(w) \in \{1, 2\}$ in which case $\left(\prod_{t=1}^{q-1}(y_t)^{a_t}\right)\left((y_q)^c(w)\right) \in \{1, 2\}$. Otherwise $\left(\prod_{t=1}^{q-1}(y_t)^{a_t}\right)\left((y_q)^c(w)\right) = (y_1)^{a_1}\left((y_q)^c(w)\right) = (y_q)^c(w) \neq n$. □

The next simplest class of nonabelian simple groups are the groups denoted in [5] by $A_n(q)$.

3.21 Definition.

(a) Let F be a field and let $m \in \mathbb{N}$. Then $GL_m(F)$ is the set of all $m \times m$ matrices over F with nonzero determinant.

(b) Let F be a field and let $m \in \mathbb{N}$. Then $SL_m(F) = \{w \in GL_m(F) : \det(w) = 1\}$.

(c) Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, let F be the field with q elements, and let Z be the center of $SL_{m+1}(F)$. Then $A_m(q) = SL_{m+1}(F)/Z$ and $\pi_m : SL_{m+1}(F) \to A_m(q)$ is the quotient map.

(d) Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, and let F be the field with q elements. Then $W_m(q) = \{w \in SL_{m+1}(F) : \text{for all } t \in \{2, 3, \ldots, m+1\},\ w_{t,1} = 0\}$.

The following lemma is well known and its proof is at any rate an easy exercise.

3.22 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, let F be the field with q elements, and let Z be the center of $SL_{m+1}(F)$. Let $D = \{x \in F : x^{m+1} = 1\}$ and let I be the $(m+1) \times (m+1)$ identity matrix. Then $Z = \{xI : x \in D\}$ and $|D| = \gcd(m+1, q-1)$.*

According to [12] all of the nonabelian simple groups of order less than 6000 are of the form A_n, $A_1(p^k)$, or $A_2(p^k)$.

We saw above that each A_n has a strong digital representation. The smaller simple groups not of this form are (with order in parentheses) $A_1(7)$ $(168 = 2^3 \cdot 3 \cdot 7)$, $A_1(8)$ $(504 = 2^3 \cdot 3^2 \cdot 7)$, $A_1(11)$ $(660 = 2^2 \cdot 3 \cdot 5 \cdot 11)$, $A_1(13)$ $(1092 = 2^2 \cdot 3 \cdot 7 \cdot 13)$, $A_1(17)$ $(2448 = 2^4 \cdot 3^2 \cdot 17)$, $A_1(19)$ $(3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19)$, $A_1(16)$ $(4080 = 2^4 \cdot 3 \cdot 5 \cdot 17)$, and $A_2(3)$ $(5616 = 2^4 \cdot 3^3 \cdot 13)$.

The following lemma, except possibly for part (d), is well known.

3.23 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, and let F be the field with q elements.*

(a) $|GL_{m+1}(F)| = q^{m(m+1)/2} \prod_{t=0}^{m}(q^{t+1} - 1)$.

(b) $|SL_{m+1}(F)| = q^{m(m+1)/2} \prod_{t=1}^{m}(q^{t+1} - 1)$.

(c) If $d = \gcd(m+1, q-1)$, *then* $|A_m(q)| = \frac{1}{d} q^{m(m+1)/2} \prod_{t=1}^{m}(q^{t+1} - 1)$.

(d) $|W_m(q)| = q^{m(m+1)/2} \prod_{t=0}^{m-1}(q^{t+1} - 1)$.

Proof. (a) To obtain a matrix in $GL_{m+1}(F)$ the first row can be any nonzero vector in F^{m+1} and in general for $i \in \{1, 2, \ldots, m\}$, row $i+1$ can be any row not in the linear span of the first i rows, so

$$\begin{aligned} |GL_{m+1}(F)| &= \textstyle\prod_{t=0}^{m}(q^{m+1} - q^t) \\ &= \textstyle\prod_{t=0}^{m} q^t \prod_{t=0}^{m}(q^{m+1-t} - 1) \\ &= q^{m(m+1)/2} \textstyle\prod_{t=0}^{m}(q^{t+1} - 1)\,. \end{aligned}$$

(b) $|SL_{m+1}(F)| = \frac{1}{q-1}|GL_{m+1}(F)|$.

(c) This follows from (b) and Lemma 3.22.

(d) Any matrix $B \in W_m(q)$ may be written in block form as $B = \begin{pmatrix} b_{1,1} & \vec{v} \\ \vec{0} & C \end{pmatrix}$ where C is an arbitrary member of $GL_m(F)$, $\vec{v}$ is an arbitrary member of F^m, and $b_{1,1} = (\det C)^{-1}$. Consequently, $|W_m(q)| = q^m \cdot |GL_m(F)|$. □

3.24 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, and let $n = \sum_{t=0}^{m} q^t$. Then* $\gcd(n, q-1) = \gcd(m+1, q-1)$.

Proof. We have that $n = (m+1) + \sum_{t=1}^{m}(q^t - 1)$ and $q-1$ divides $q^t - 1$ for each $t \in \{1, 2, \ldots, m\}$. Therefore any power of a prime which divides $q-1$ divides n if and only if it divides $m+1$. □

It is a fact, apparently due to Gauss [4] who counted all such things, though this fact may predate that, that given any $m \geq 2$ and any finite field F there is an irreducible polynomial of degree m over F. In fact the following holds.

3.25 Lemma. *Let F be a finite field, let $\widetilde{F}$ be a field extension of degree m over F, and let ξ be a generator of the (cyclic) multiplicative group of $\widetilde{F}$. There is an irreducible polynomial f of degree m over F such that ξ is a root of f in $\widetilde{F}$.*

Proof. [11, Theorem 2.10 and Corollary 2.11]. □

3.26 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, let F be the field with q elements and let f be an irreducible polynomial of degree $m+1$ over F. Let $\widetilde{F}$ be the field obtained by adjoining a root ξ of f to F. Given $\eta \in \widetilde{F} \setminus \{0\}$, multiplication by η is a linear transformation from $\widetilde{F}$ to itself; let $\phi_{m,f}(\eta)$ be the matrix representation of this linear transformation with respect to the basis $\{1, \xi, \xi^2, \ldots, \xi^m\}$ for $\widetilde{F}$ as a vector space over F. Then $\phi_{m,f}$ is an injective homomorphism from the multiplicative group of $\widetilde{F}$ to $GL_{m+1}(F)$.*

Proof. Given $\eta \in \widetilde{F} \setminus \{0\}$, $\big(\phi_{m,f}(\eta)\big)^{-1} = \phi_{m,f}(\eta^{-1})$ and so $\det\big(\phi_{m,f}(\eta)\big) \neq 0$. □

3.27 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$, let $q = p^k$, let F be the field with q elements and let f be an irreducible polynomial of degree $m+1$ over F. Let $\widetilde{F}$ be the field obtained by adjoining a root ξ of f to F and let $n = \sum_{t=0}^{m} q^t$. Let $\phi_{m,f}$ be defined as in Lemma* 3.26. *Let $\widetilde{F}^*$ be the multiplicative group of $\widetilde{F}$ and let $X = \{\eta^{q-1} : \eta \in \widetilde{F}^*\}$. Then X is a subgroup of $\widetilde{F}^*$ such that $|X| = n$ and $\phi_{m,f}[X] \subseteq SL_{m+1}(F)$.*

Proof. Pick a generator δ of $\widetilde{F}$. Then $X = \big\{\delta^{t(q-1)} : t \in \{1, 2, \ldots, n\}\big\}$ so $|X| = n$. To see that $\phi_{m,f}[X] \subseteq SL_{m+1}(F)$, let $t \in \{1, 2, \ldots, n\}$. Then $1 = \Big(\det\big(\phi_{m,f}(\delta^t)\big)\Big)^{q-1} = \det\big(\phi_{m,f}(\delta^{t(q-1)})\big)$. □

3.28 Lemma. *Let p be a prime, let $k, m \in \mathbb{N}$ with $m > 1$, let $q = p^k$, and let F be the field with q elements. If $A_{m-1}(q)$ has a strong digital representation, then so do $SL_m(F)$ and $\pi_m[W_m(q)]$.*

Proof. Assume that $A_{m-1}(q)$ has a strong digital representation. The center of $SL_m(F)$ is abelian so has a strong digital representation by Theorem 3.9 and thus so does $SL_m(F)$ by Theorem 3.4.

Let F^* be the multiplicative subgroup of F and let $D = \{a \in F^* : a^{m+1} = 1\}$. Define $\psi : \pi_m[W_m(q)] \to F^*/D$ by, for $x \in W_m(q)$, $\psi\big(\pi_m(z)\big) = z_{1,1}D$. Then ψ is a well defined surjective homomorphism and F^*/D is abelian and thus has a strong digital representation by Theorem 3.9. Consequently by Theorem 3.4 it suffices to show that the kernel of ψ has a strong digital representation.

Let $U = \{z \in W_m(q) : z_{1,1} = 1\}$. Given $z \in U$, let $\tau(z)$ be the lower right $m \times m$ corner of z. Then τ is a homomorphism from U onto $SL_m(F)$ and z is in the kernel of τ if and only if there is some $\vec{v} \in F^q$ such that

$$z = \begin{pmatrix} 1 & \vec{v} \\ \vec{0} & I \end{pmatrix}$$

where I is the $m \times m$ identity matrix. Thus the kernel of τ is abelian so has a strong digital representation, and since $SL_m(F)$ has a strong digital representation, so does U. Finally, the restriction of π_m to U is an isomorphism onto the kernel of ψ. □

3.29 Theorem. *Let p be a prime, let $k, m \in \mathbb{N}$, and let $q = p^k$. Then $A_m(q)$ has a strong digital representation.*

Proof. Let F be the field with q elements. We proceed by induction on m. We ground

the induction by showing that $\pi_1[W_1(q)]$ has a strong digital representation. Let

$$K = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in F \setminus \{0\} \right\} \text{ and } M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in F \text{ and } a^2 = 1 \right\}.$$

Then $W_1(q) = KM$ so $\pi_1[W_1(q)] = \pi_1[K]\pi_1[M]$. Also K is abelian and so $\pi_1[K]$ is abelian so has a strong digital representation by Theorem 3.9. Since $|\pi_1[M]| = q$ we have by Theorem 3.12 that $\pi_1[M]$ has a strong digital representation. Since $\pi_1[M] \cap \pi_1[K] = \{\pi_1[I]\}$ we have by Lemma 3.1 that $\pi_1[W_1(q)]$ has a strong digital representation.

Let $m \in \mathbb{N}$ and assume that $\pi_m[W_m(q)]$ has a strong digital representation. We shall show that $A_m(q)$ has a strong digital representation and so, by Lemma 3.28, the same is true for $\pi_{m+1}[W_{m+1}(q)]$.

Pick by Lemma 3.25 an irreducible polynomial f of degree $m+1$ over F such that one may represent the field $\widetilde{F}$ of degree $m+1$ over F as the vector space with basis $\{1, \xi, \xi^2, \ldots, \xi^m\}$ where ξ is a root of f and a generator of the multiplicative group $\widetilde{F}^*$ of $\widetilde{F}$. Let $d = \gcd(m+1, q-1)$. We define an element $v \in SL_{m+1}(F)$ as follows:

(a) If $d = 1$, let $v = I$, the $(m+1) \times (m+1)$ identity matrix.

(b) If d is odd and $d > 1$, then let $v_{1,d} = 1$, let $v_{i,i-1} = 1$ for $i \in \{2, 3, \ldots, d\}$, and let $v_{i,i} = 1$ for $i \in \{d+1, d+2, \ldots, m+1\}$. Let all other entries of v be 0. (Thus v is obtained from I by permuting the first d rows of I via the cycle $(1, 2, \ldots, d)$. Since this is an even permutation, $\det(v) = 1$.)

(c) If d is even and $d < m+1$, then let $v_{1,d} = 1$, let $v_{i,i-1} = 1$ for $i \in \{2, 3, \ldots, d\}$, let $v_{i,i} = 1$ for $i \in \{d+1, d+2, \ldots, m\}$, and let $v_{m+1,m+1} = -1$. Let all other entries of v be 0.

(d) If d is even and $d = m+1$, then let $v_{1,d} = -1$ and let $v_{i,i-1} = 1$ for $i \in \{2, 3, \ldots, m+1\}$.

Let V be the subgroup of $SL_{m+1}(F)$ generated by v. In the first three cases, $|V| = d$ and $V \cap W_m(q) = V \cap Z\big(SL_{m+1}(F)\big) = \{I\}$, where $Z\big(SL_{m+1}(F)\big)$ is the center of $SL_{m+1}(F)$, so that $|\pi_m[V]| = d$. In the last case, $|V| = 2d$ and $V \cap W_m(q) = V \cap Z\big(SL_{m+1}(F)\big) = \{I, -I\}$ so that again $|\pi_m[V]| = d$.

Let $n = \sum_{t=0}^{m} q^t$, let $\phi_{m,f}$ be defined as in Lemma 3.26, and let $X = \big\{\xi^{t(q-1)} : t \in \{1, 2, \ldots, n\}\big\}$. Then, by Lemma 3.27, X is a subgroup of $\widetilde{F}^*$ and $\phi_{m,f}[X] \subseteq SL_{m+1}(F)$.

We now claim that $VW_m(q)V \cap \phi_{m,f}[X] \subseteq Z\big(SL_{m+1}(F)\big)$. To see this, let $\eta \in X$ and assume that $\phi_{m,f}(\eta) \in VW_m(q)V$. Pick $y, z \in V$ and $w \in W_m(q)$ such that $\phi_{m,f}(\eta) = ywz$. Then yw is obtained from w by permuting the first d rows and possibly multiplying some rows by -1. So we may pick $i \in \{1, 2, \ldots, d\}$ such that the only

nonzero entry of column 1 of yw is in row i. Now ywz is obtained from yw by permuting the first d columns and possibly multiplying some columns by -1. Thus there is some $j \in \{1, 2, \ldots, d\}$ such that the entry in row i and column j of ywz is some $b \neq 0$ and all other entries of column j are 0. Thus if u is the column vector with j^{th} entry equal to 1 and all other entries 0 one has that $\phi_{m,f}(\eta)u$ is the column vector with i^{th} entry equal to b and all other entries 0. That is, $\eta\xi^j = b\xi^i$. Thus $\xi^{i-j} = b^{-1}\eta$. Now $b^{-1} = \xi^s$ for some $s \in \{1, 2, \ldots, q^{m+1}\}$ and $\eta = \xi^{t(q-1)}$ for some $t \in \{1, 2, \ldots, n\}$. Thus $\xi^{i-j} = \xi^{s+t(q-1)}$. Now $1 = b^{1-q} = \xi^{s(1-q)}$ and so $n(q-1) = q^{m+1} - 1$ divides $s(q-1)$ and thus n divides s. By Lemma 3.24 d divides n and thus d divides s. Also d divides $q-1$ and so d divides $s + t(q-1)$ and thus d divides $i - j$. Since $-d < i - j < d$ we have that $i = j$ and thus $\eta = b \in F$. We then have that $\phi_{m,f}(\eta) = bI$ and since $\det\big(\phi_{m,f}(\eta)\big) = 1$, $\phi_{m,f}(\eta) \in Z\big(SL_{m+1}(F)\big)$, as claimed.

We have that $\pi_m[W_m(q)]$ has a strong digital representation by the induction hypothesis. Also, $\phi_{m,f}[X]$ is commutative by Lemma 3.26 and so $\pi_m[V]$ and $\pi_m\big[\phi_{m,f}[X]\big]$ are commutative and so have strong digital representations by Theorem 3.9. By Lemma 3.23 and the fact that $Z\big(SL_{m+1}(F)\big) \subseteq W_m(q)$ we have that

$$|\pi_m[W_m(q)]| = \tfrac{1}{d} q^{m(m+1)/2} \textstyle\prod_{t=0}^{m-1}(q^{t+1} - 1)$$

while $|\pi_m[V]| = d$ and $\big|\pi_m\big[\phi_{m,f}[X]\big]\big| \geq \frac{n}{d}$ so $|\pi_m[W_m(q)]| \cdot |\pi_m[V]| \cdot \big|\pi_m\big[\phi_{m,f}[X]\big]\big| \geq \frac{1}{d} q^{m(m+1)/2} \prod_{t=1}^{m}(q^{t+1} - 1) = |A_m(q)|$. Thus it suffices to show that if $w_1, w_2 \in W_m(q)$, $y_1, y_2 \in V$, $z_1, z_2 \in \phi_{m,f}[X]$, and $\pi_m(w_1)\pi_m(y_1)\pi_m(z_1) = \pi_m(w_2)\pi_m(y_2)\pi_m(z_2)$, then $\pi_m(w_1) = \pi_m(w_2)$, $\pi_m(y_1) = \pi_m(y_2)$, and $\pi_m(z_1) = \pi_m(z_2)$.

So assume that we have $\pi_m(w_1)\pi_m(y_1)\pi_m(z_1) = \pi_m(w_2)\pi_m(y_2)\pi_m(z_2)$. Then there is some $u_1 \in Z\big(SL_{m+1}(F)\big)$ such that $(z_2)^{-1}(y_2)^{-1}(w_2)^{-1}w_1y_1z_1 = u_1$ so

$$z_2z_1^{-1} = (y_2)^{-1}(w_2)^{-1}(u_1)^{-1}w_1y_1z_1 \in VW_m(q)V \cap \phi_{m,f}[X]$$

so there is some $u_2 \in Z\big(SL_{m+1}(F)\big)$ such that $z_2z_1^{-1} = u_2$ and in particular $\pi_m(z_1) = \pi_m(z_2)$. Now $y_2(y_1)^{-1} = (w_2)^{-1}(u_2)^{-1}(u_1)^{-1}w_1 \in V \cap W_m(q)$ so $\pi_m(y_2) = \pi_m(y_1)$ and then $\pi_m(w_2) = \pi_m(w_1)$. □

4. Applications to semigroup compactifications

In this section we shall show that, for a class of discrete semigroups S which includes all infinite abelian groups, the smallest ideal of βS contains copies of the free group on $2^{2^{|S|}}$ generators; and that, for any infinite discrete abelian group S, the weakly almost

periodic compactification of S contains copies of the free abelian semigroup on $2^{2^{|S|}}$ generators.

Given a discrete semigroup $(S, \cdot)$, we take the Stone-Čech compactification βS of S to be the set of ultrafilters on S, identifying the points of S with the principal ultrafilters and thus pretending that $S \subseteq \beta S$. Given $A \subseteq S$ and $p \in \beta S$, $A \in p$ if and only if $p \in cl_{\beta S} A$. The operation extends to βS making $(\beta S, \cdot)$ a right topological semigroup (meaning that for each $p \in \beta S$, the function $\rho_p : \beta S \to \beta S$ defined by $\rho_p(q) = q \cdot p$ is continuous) with S contained in its topological center (meaning that for each $s \in S$, the function $\lambda_s : \beta S \to \beta S$ defined by $\lambda_s(q) = s \cdot q$ is continuous). Given $p, q \in \beta S$,

$$p \cdot q = \lim_{\substack{s \to p \\ s \in S}} \lim_{\substack{t \to q \\ t \in S}} s \cdot t \,.$$

Thus if $p, q \in \beta S$ and $A \subseteq S$, then $A \in p \cdot q$ if and only if $\{s \in S : s^{-1}A \in q\} \in p$ where $s^{-1}A = \{t \in S : s \cdot t \in A\}$.

If T is any compact right topological semigroup, it has a smallest two sided ideal $K(T)$ which is the union of all of the minimal right ideals of T and is also the union of all of the minimal left ideals of T. If L is a minimal left ideal and R is a minimal right ideal, then $L \cap R$ is a group, and any two such groups are isomorphic. A given copy of this group is called the *structure group* of T. If p is an idempotent in T, L is the minimal left ideal with $p \in L$ and R is the minimal right ideal with $p \in R$, then $L \cap R = pTp$. See [9] for a gentle introduction to βS and its algebraic structure.

Under reasonable hypotheses the structure group of βS is known to be quite rich. For example, the structure group of $(\beta\mathbb{N}, +)$ contains a copy of the free group on $2^{\mathfrak{c}}$ generators [9, Corollary 7.37] (a fact originally established in [8]). (Recall that $|\beta\mathbb{N}| = 2^{\mathfrak{c}}$.) Further, if G is a countably infinite group which can be mapped into a compact metrizable topological group by an injective homomorphism, then the structure group of βG contains a copy of the free group on $2^{\mathfrak{c}}$ generators [9, Corollary 7.40].

It is also known that if S is a weakly left cancellative and right cancellative semigroup with $|S| = \kappa \geq \omega$, then βS contains a copy of the free group on 2^{2^κ} generators [9, Corollary 7.39]. The proof given in [9] is, in fact, valid for the larger class of semigroups which are weakly left cancellative and nearly right cancellative. (A semigroup S is said to be nearly right cancellative if there is a subset D of S such that $|D| = |S|$ and for every distinct $s, t \in S$, $\{d \in D : sd = td\}$ is finite. There are many examples of semigroups which arise very naturally and are weakly left cancellative and nearly right cancellative, but not right cancellative. These include $(\mathcal{P}_f(X), \cup)$, where X is an arbitrary set, $(\mathbb{N}, \max)$ and $(\mathbb{N}, \text{lcm})$. The concept of near right cancellativity was

introduced in [3] and is discussed there.) However, [9, Corollary 7.39] provides no information about the structure group of $K(\beta S)$, as the free groups constructed in this theorem do not normally meet $K(\beta S)$.

In this section we show that if S is a semigroup with $|S| = \kappa \geq \omega$ which has a digital representation and satisfies a related commutavity condition, then there is a compact subsemigroup V of βS whose structure group contains a copy of the free group on 2^{2^κ} generators. We show that if, in addition, S is left cancellative, then the structure group of βS contains a copy of the free group on 2^{2^κ} generators. As a corollary, we show that if T is any semigroup which has as a homomorphic image a commutative cancellative semigroup of cardinality κ with a digital representation, then the structure group of βT contains a copy of the free group on 2^{2^κ} generators.

4.1 Convention. *We shall assume througout this section until Corollary* 4.16 *that* $(S, \cdot)$ *is a semigroup with identity* 1 *and cardinality* κ *which has a digital representation* $\langle F_t \rangle_{t \in \kappa}$. *We shall also assume that if* $s < t < \kappa$, $x \in F_t$, *and* $y \in F_s$, *then* $xy = yx$.

We remark that our assumptions are satisfied if S is a commutative group (by Theorem 3.9) or if S is a semigroup which is a direct sum of finite semigroups with identities.

4.2 Definition.

(a) We put $\text{supp}(1) = \emptyset$. If $s = \prod_{t \in H} x_t$ where each $x_t = F_t$, let $\text{supp}(s) = H$.

(b) If $a, b \in S$, we write $a \perp b$ if $\text{supp}(a) \cap \text{supp}(b) = \emptyset$.

(c) For $J \subseteq \kappa$, $D_J = \{s \in S : \text{supp}(s) \cap J = \emptyset\}$.

(d) $V = \bigcap_{J \in \mathcal{P}_f(\kappa)} c\ell_{\beta S} D_J$.

(e) $C = \bigcap \{c\ell_{\beta S} D_J : J \subseteq \kappa \text{ and } |J| < \kappa\}$.

Notice that Convention 4.1 guarantees that if $a, b \in S$ and $a \perp b$, then $ab = ba$ and $\text{supp}(ab) = \text{supp}(a) \cup \text{supp}(b)$.

We remark that if $(S, \cdot) = (\mathbb{N}, +)$ and $F_t = \{2^t\}$ for $t < \omega$, then $V = C = \bigcap_{t=0}^{\infty} c\ell_{\beta \mathbb{N}} (2^t \mathbb{N}) = \mathbb{H}$, a subsemigroup of $\beta \mathbb{N}$ which includes all of the idempotents of $\beta \mathbb{N}$ and has substantial known structure. See [9, Sections 6.3 and 7.2] for information about the structure of $\mathbb{H}$ and where its copies may be found.

4.3 Lemma. *Both* V *and* C *are subsemigroups of* βS.

Proof. For V, let $\mathcal{A} = \mathcal{P}_f(\kappa)$. For C, let $\mathcal{A} = \{J \subseteq \kappa : |J| < \kappa\}$. By [9, Theorem 4.20] it suffices to observe that if $J \in \mathcal{A}$ and $s \in D_J$, then for all $t \in D_{J \cup \text{supp}(s)}$, $s \cdot t \in D_J$. □

We set out to show that maximal subgroups in the smallest ideal of V contain copies of the free group on 2^{2^κ} generators. The proof of Theorem 4.4 will include several subsidiary lemmas.

4.4 Theorem. *Let p be an idempotent in $K(V)$. The group pVp contains a copy of the free group on 2^{2^κ} generators.*

Proof. Choose $b_t \in F_t$ for each $t \in I$ and let U be the set of uniform ultrafilters on $\{b_t : t < \kappa\}$. Then it is well known that $|U| = 2^{2^\kappa}$. (See for example [9, Theorem 3.58].) Enumerate U as $\{r_t : t < 2^{2^\kappa}\}$. Let T be the free group on the generators $\{\alpha_t : t < 2^{2^\kappa}\}$ with identity 1 and let $\varphi : T \to pVp$ be the unique homomorphism such that $\varphi(1) = p$ and $\varphi(\alpha_t) = pr_tp$ for each $t < 2^{2^\kappa}$.

It suffices to show that the kernel of φ is $\{1\}$ so suppose instead there is some other element in the kernel. Choose $d \in \mathbb{N}$, $w_1, w_2, \ldots, w_d$ in pVp, and $l_1, l_2, \ldots, l_d$ in $\mathbb{N}$ such that for each $i \in \{1, 2, \ldots, d\}$ there exists $t(i) < 2^{2^\kappa}$ such that either $w_i = pr_{t(i)}p$ or $w_i = (pr_{t(i)}p)^{-1}$, $t(i) \neq t(i+1)$ if $i < d$, and $(w_1)^{l_1} \cdot (w_2)^{l_2} \cdots (w_d)^{l_d} = p$. Let $n = \big|\big\{t(i) : i \in \{1, 2, \ldots, d\}\big\}\big|$ and let $\{x_1, x_2, \ldots, x_n\} = \big\{r_{t(i)} : i \in \{1, 2, \ldots, d\}\big\}$. Choose a partition $\{J_1, J_2, \ldots, J_n\}$ of κ such that $\{b_t : t \in J_i\} \in x_i$ for each $i \in \{1, 2, \ldots, n\}$. Let $M = 1 + \prod_{i=1}^{d} l_i$.

Let E be the set of finite sequences in $\{1, 2, \ldots, n\}$ including the empty sequence. Let $[\kappa]^{<\omega}$ be the set of finite subsets of κ (so $[\kappa]^{<\omega} = \mathcal{P}_f(\kappa) \cup \{\emptyset\}$). Define $\psi : [\kappa]^{<\omega} \to E$ as follows. First $\psi(\emptyset) = \emptyset$. If $\mu \in \mathcal{P}_f(\kappa)$ and $\mu = \{j_1, j_2, \ldots, j_k\}$ where $j_1 < j_2 < \ldots < j_k$, then for $i \in \{1, 2, \ldots, k\}$ let a_i be the member of $\{1, 2, \ldots, n\}$ such that $j_i \in J_{a_i}$. Then $\psi(\mu) = \langle a_1, a_2, \ldots, a_k \rangle$.

Given $\sigma \in E$ and $s \in S$, let $\phi_\sigma(s) = \{\mu \subseteq \mathrm{supp}(s) : \psi(\mu) = \sigma\}$. Define for $\sigma \in E$, $\delta_\sigma : S \to \mathbb{Z}_M$ by $\delta_\sigma(s) \equiv |\phi_\sigma(s)| \pmod M$ and let $\widetilde{\delta}_\sigma : \beta S \to \mathbb{Z}_M$ be the continuous extension of δ_σ. We shall (eventually) show that there is some $\sigma \in E$ such that $\widetilde{\delta}_\sigma\big((w_1)^{l_1} \cdot (w_2)^{l_2} \cdots (w_d)^{l_d}\big) \neq \widetilde{\delta}_\sigma(p)$, which will complete the proof.

For $J \subseteq \kappa$, define $\gamma_J : S \to \mathbb{Z}_M$ by $\gamma_J(s) \equiv |\mathrm{supp}(s) \cap J| \pmod M$ and let $\widetilde{\gamma}_J : \beta S \to \mathbb{Z}_M$ be the continuous extension of γ_J.

4.5 Lemma. *Let $h : \beta S \to R$ be a continuous mapping into a compact right topological semigroup. If $h(ab) = h(a)h(b)$ for every $a, b \in S$ such that $a \perp b$, then $h(xv) = h(x)h(v)$ for every $x \in \beta S$ and every $v \in V$, and so the restriction of h to V is a homomorphism. In particular, for any $J \subseteq \kappa$, the restriction of $\widetilde{\gamma}_J$ to V is a homomorphism. If $i \in \{1, 2, \ldots, n\}$ and $\sigma = \langle i \rangle$, then $\delta_\sigma = \gamma_{J_i}$ so the restriction of $\widetilde{\delta}_\sigma$ to V is a homomorphism.*

Proof. We have $h(xv) = \lim_{a\to x}\lim_{b\to v} h(ab) = \lim_{a\to x}\lim_{b\to v} h(a)h(b) = h(x)h(v)$.

For the last assertion note that given $s \in S$, $\mu \in \phi_\sigma(s)$ if and only if there is some $j \in \operatorname{supp}(s) \cap J_i$ such that $\mu = \{j\}$. □

4.6 Lemma. *Let r be an idempotent in V and for each $\mu \in [\kappa]^{<\omega}$ let $R_\mu \in r$. For $k \in \mathbb{N}$ and $\mu \in [\kappa]^{<\omega}$ let*

$$B_{\mu,k} = \big\{s_1 \cdot s_2 \cdots s_k : \text{for } i \in \{1,2,\ldots,k\}\,, \operatorname{supp}(s_i) \cap \mu = \emptyset\,, \operatorname{supp}(s_i) \cap \operatorname{supp}(s_j) = \emptyset \text{ when } i \neq j\,,\ s_1 \in \bigcap\{R_\nu : \nu \subseteq \mu\}, \text{ and for } t \in \{2,3,\ldots,k\}\,,\ s_t \in \bigcap\{R_\nu : \nu \subseteq \mu \cup \operatorname{supp}(s_1 \cdot s_2 \cdots s_{t-1})\}\big\}\,.$$

Then each $B_{\mu,k} \in r$.

Proof. We proceed by induction on k. If $\mu \in [\kappa]^{<\omega}$, then

$$B_{\mu,1} = D_\mu \cap \big(\bigcap\{R_\nu : \nu \subseteq \mu\}\big) \in r\,.$$

So let $k \in \mathbb{N}$ and assume that the assertion holds for k.

Let $\mu \in [\kappa]^{<\omega}$. We claim that $D_\mu \cap \big(\bigcap\{R_\nu : \nu \subseteq \mu\}\big) \subseteq \{s \in S : s^{-1}B_{\mu,k+1} \in r\}$ so that $B_{\mu,k+1} \in r \cdot r = r$. So let $x_1 \in D_\mu \cap \big(\bigcap\{R_\nu : \nu \subseteq \mu\}\big)$. We claim that $D_{\operatorname{supp}(x_1)} \cap B_{\mu\cup\operatorname{supp}(x_1),k} \subseteq (x_1)^{-1}B_{\mu,k+1}$. So let $s_1 \cdot s_2 \cdots s_k \in D_{\operatorname{supp}(x_1)} \cap B_{\mu\cup\operatorname{supp}(x_1),k}$ where for $i \in \{1,2,\ldots,k\}$, $\operatorname{supp}(s_i) \cap \big(\mu \cup \operatorname{supp}(x_1)\big) = \emptyset$, $\operatorname{supp}(s_i) \cap \operatorname{supp}(s_j) = \emptyset$ when $i \neq j$, $s_1 \in \bigcap\{R_\nu : \nu \subseteq \mu \cup \operatorname{supp}(x_1)\}$, and for $t \in \{2,3,\ldots,k\}$

$$s_t \in \bigcap\{R_\nu : \nu \subseteq \mu \cup \operatorname{supp}(x_1) \cup \operatorname{supp}(s_1 \cdot s_2 \cdots s_{t-1})\}\,.$$

For $t \in \{2,3,\ldots,k+1\}$, let $x_t = s_{t-1}$. Then $x_1 \cdot x_2 \cdots x_{k+1} \in B_{\mu,k+1}$. □

4.7 Lemma. *Let $\sigma \in E$, let r be an idempotent in V, and let*

$$L = \{\mu \in [\kappa]^{<\omega} : \psi(\mu) \text{ is a subsequence of } \sigma\}\,.$$

For $\mu \in L$ and $s \in S$, let $\theta_\mu(s) = \{\nu \subseteq \operatorname{supp}(s) : \mu \cap \nu = \emptyset \text{ and } \mu \cup \nu \in L\}$. Then for all $m \in \mathbb{N}$ and all $\mu \in L$, there is some $R \in r$ such that for all $s \in R$, $|\{\nu \in \theta_\mu(s) : |\nu| = m\}| \equiv 0 \pmod M$.

Proof. If $\sigma = \emptyset$, then $L = \{\emptyset\}$ and $\theta_\mu(s) = \{\emptyset\}$ for all $s \in S$ so the conclusion holds. We shall assume that $\sigma \neq \emptyset$ and proceed by induction on m. Assume first that $m = 1$. Let $\mu \in L$ and let $J = \{t < \kappa : t \notin \mu \text{ and } \mu \cup \{t\} \in L\}$. By Lemma 4.5 the restriction of $\widetilde{\gamma}_J$ to V is a homomorphism so $\widetilde{\gamma}_J(r) = 0$ so pick $R \in r$ such that for all $s \in R$, $\gamma_J(s) = 0$. Given $s \in R$, $\{\nu \in \theta_\mu(s) : |\nu| = 1\} = \big\{\{t\} : t \in \operatorname{supp}(s) \cap J\big\}$ so $|\{\nu \in \theta_\mu(s) : |\nu| = 1\}| \equiv \gamma_J(s) \pmod M$.

Now let $m > 1$ and assume that the result holds for all $k < m$. For each $\mu \in L$, pick $R_\mu \in r$ such that for all $k < m$ and all $s \in R_\mu$, $|\{\nu \in \theta_\mu(s) : |\nu| = k\}| \equiv 0 \pmod{M}$. If $\mu \in [\kappa]^{<\omega} \setminus L$, let $R_\mu = S$.

Let $\mu \in L$ be given and pick $a \in \mathbb{Z}_M$ and $R' \in r$ such that for all $s \in R'$, $|\{\nu \in \theta_\mu(s) : |\nu| = m\}| \equiv a \pmod{M}$. Define $B_{\mu,M}$ as in Lemma 4.6 and let $R = B_{\mu,M} \cap R' \cap \left(\bigcap\{R_\nu : \nu \subseteq \mu\}\right)$. Then $R \in r$. Let $t \in R$ and let $H = \{\nu \in \theta_\mu(t) : |\nu| = m\}$. We shall show that $|H| \equiv 0 \pmod{M}$. Pick $s_1, s_2, \ldots, s_M$ as guaranteed by the definition of $B_{\mu,M}$ such that $t = s_1 \cdot s_2 \cdots s_M$.

Suppose that $t \in R$ satisfies $t = s_1 \cdot s_2 \cdots s_M$, where $s_1, s_2, \ldots, s_M$ have properties (i), (ii), and (iii). Let $H = \{\nu \in \theta_\mu(t) : |\nu| = m\}$. We shall show that $|H| \equiv 0 \pmod{M}$.

If $i \in \{1, 2, \ldots, M\}$, then since $t \in R'$, $|H \cap \theta_\mu(s_i)| \equiv a \pmod{M}$ and so

$$\left|\bigcup_{i=1}^{M} \left(H \cap \theta_\mu(s_i)\right)\right| \equiv aM \equiv 0 \pmod{M}.$$

Given $A \subseteq \{1, 2, \ldots, M\}$ such that $|A| \geq 2$, let

$$H_A = \left\{\nu \in H : A = \{i \in \{1, 2, \ldots, M\} : \nu \cap \operatorname{supp}(s_i) \neq \emptyset\}\right\}.$$

Then $H = \bigcup_{i=1}^{M} \left(H \cap \theta_\mu(s_i)\right) \cup \bigcup\{H_A : A \subseteq \{1, 2, \ldots, M\} \text{ and } |A| \geq 2\}$ and the listed sets are pairwise disjoint so it suffices to let $A \subseteq \{1, 2, \ldots, M\}$ such that $|A| \geq 2$ and show that $|H_A| \equiv 0 \pmod{M}$.

Let $c = \max A$ and let $v = \prod_{i \in A \setminus \{c\}} s_i$. Let

$$K = \{\gamma \in \theta_\mu(v) : \text{ for each } i \in A \setminus \{c\}, \gamma \cap \operatorname{supp}(s_i) \neq \emptyset \text{ and } |\gamma| = m\}$$

and for $\gamma \in K$, let $T_\gamma = \{\tau \in \theta_{\mu \cup \gamma}(s_c) : |\tau| = m - |\gamma|\}$. We claim that $H_A = \bigcup_{\gamma \in K} \{\gamma \cup \tau : \tau \in T_\gamma\}$. This will suffice because:

(a) if $\gamma, \gamma' \in K$ and $\gamma \neq \gamma'$, then $\{\gamma \cup \tau : \tau \in T_\gamma\} \cap \{\gamma' \cup \tau : \tau \in T_{\gamma'}\} = \emptyset$ since $(\gamma \cup \tau) \cap \operatorname{supp}(v) = \gamma$;

(b) for $\gamma \in K$, $|\{\gamma \cup \tau : \tau \in T_\gamma\}| = |T_\gamma|$; and

(c) for $\gamma \in K$, since $s_c \in R_{\mu \cup \gamma}$, $|\{\tau \in \theta_{\mu \cup \gamma}(s_c) : |\tau| = m - |\gamma|\}| \equiv 0 \pmod{M}$, i.e., $|T_\gamma| \equiv 0 \pmod{M}$.

To see that $H_A \subseteq \bigcup_{\gamma \in K} \{\gamma \cup \tau : \tau \in T_\gamma\}$, let $\nu \in H_A$. Let $\gamma = \nu \cap \operatorname{supp}(v)$ and let $\tau = \nu \cap \operatorname{supp}(s_c)$. Then $\gamma \in \theta_\mu(t)$ because $\gamma \subseteq \nu$ so that $\gamma \cup \mu \subseteq \nu \cup \mu$ and thus $\psi(\gamma \cup \mu)$ is a subsequence of $\psi(\nu \cup \mu)$. Consequently $\gamma \cup \mu \in L$ so that $\gamma \in \theta_\mu(v)$ and thus $\gamma \in K$. Also $\mu \cup \gamma \cup \tau = \mu \cup \nu$ so $\tau \in \theta_{\mu \cup \gamma}(s_c)$. Since $|\nu| = m$, $\tau \in T_\gamma$.

To see that $\bigcup_{\gamma \in K} \{\gamma \cup \tau : \tau \in T_\gamma\} \subseteq H_A$, let $\gamma \in K$ and let $\tau \in T_\gamma$. Let $\nu = \gamma \cup \tau$. Then $\psi(\mu \cup \nu) = \psi(\mu \cup \gamma \cup \tau)$ so $\nu \in \theta_\mu(t)$ and $|\nu| = m$ so $\nu \in H_A$. □

4.8 Lemma. *Let $\sigma \in E \setminus \{\emptyset\}$, let r be an idempotent in V, and let $x \in \beta S$. Then $\widetilde{\delta}_\sigma(xr) = \widetilde{\delta}_\sigma(x)$. Also $\widetilde{\delta}_\sigma(r) = 0$.*

Proof. Let L be as in the statement of Lemma 4.7. Let $a = \widetilde{\delta}_\sigma(xr)$ and let $c = \widetilde{\delta}_\sigma(x)$. Pick $B_1 \in xr$ and $B_2 \in x$ such that $\delta_\sigma[B_1] = \{a\}$ and $\delta_\sigma[B_2] = \{c\}$. Then $\{s \in S : s^{-1}B_1 \in r\} \in x$ so pick $s \in B_2$ such that $s^{-1}B_1 \in r$. Let m be the length of σ. For $\mu \in L$ and $t \in S$, let $\theta_\mu(t) = \{\nu \subseteq \text{supp}(t) : \mu \cap \nu = \emptyset \text{ and } \mu \cup \nu \in L\}$. Let $L' = \{\mu \in L : \mu \subseteq \text{supp}(s)\}$. For each $\mu \in L'$ pick by Lemma 4.7 $R_\mu \in r$ such that for each $t \in R_\mu$ and each $k \in \{1, 2, \ldots, m\}$, $|\{\nu \in \theta_\mu(t) : |\nu| = k\}| \equiv 0 \pmod{M}$. Pick $t \in s^{-1}B_1 \cap D_{\text{supp}(s)} \cap \left(\bigcap\{R_\mu : \mu \in L'\}\right)$. Now $|\phi_\sigma(s)| \equiv c \pmod{M}$. Also,

$$\phi_\sigma(st) = \phi_\sigma(s) \cup \left(\bigcup_{\mu \in L'} \{\mu \cup \nu : \nu \subseteq \text{supp}(t) \text{ and } \psi(\mu \cup \nu) = \sigma\}\right), \text{ so}$$

$$|\phi_\sigma(st)| = |\phi_\sigma(s)| + \sum_{\mu \in L'} |\{\mu \cup \nu : \nu \subseteq \text{supp}(t) \text{ and } \psi(\mu \cup \nu) = \sigma\}|.$$

For $\mu \in L'$,

$$\begin{aligned} |\{\mu \cup \nu : \nu \subseteq \text{supp}(t) \text{ and } \psi(\mu \cup \nu) = \sigma\}| &= |\{\nu \in \theta_\mu(t) : |\nu| = m - |\mu|\}| \\ &\equiv 0 \pmod{M} \end{aligned}$$

so $a = \delta_\sigma(st) \equiv |\phi_\sigma(st)| \pmod{M} \equiv |\phi_\sigma(s)| \pmod{M} \equiv c \pmod{M}$ and so $a = c$.

Putting $x = 1$ shows that $\widetilde{\delta}_\sigma(r) = 0$. □

4.9 Lemma. *Let $\sigma = \langle a_1, a_2, \ldots, a_k\rangle \in E \setminus \{\emptyset\}$, let $y \in \beta S$, and let $i \in \{1, 2, \ldots, n\}$. If $k = 1$, let $\sigma' = \emptyset$. If $k > 1$, let $\sigma' = \langle a_1, a_2, \ldots, a_{k-1}\rangle$. Then*

$$\widetilde{\delta}_\sigma(yx_i) = \begin{cases} \widetilde{\delta}_\sigma(y) & \text{if } i \neq a_k \\ \widetilde{\delta}_\sigma(y) + \widetilde{\delta}_{\sigma'}(y) & \text{if } i = a_k. \end{cases}$$

In particular, if $\sigma = \langle a_1\rangle$, then

$$\widetilde{\delta}_\sigma(yx_i) = \begin{cases} \widetilde{\delta}_\sigma(y) & \text{if } i \neq a_1 \\ \widetilde{\delta}_\sigma(y) + 1 & \text{if } i = a_1. \end{cases}$$

Proof. Pick $B \in y$ such that for all $s \in B$, $\delta_\sigma(s) = \widetilde{\delta}_\sigma(y)$ and $\delta_{\sigma'}(s) = \widetilde{\delta}_{\sigma'}(y)$. Let $A = \{sb_t : s \in B,\ t \in J_i, \text{ and } t > \max\text{supp}(s)\}$. Then $A \in yx_i$. Now let $s \in B$ and let $t > \max\text{supp}(s)$. Then $\text{supp}(sb_t) = \text{supp}(s) \cup \{t\}$. Assume first that $a_k \neq i$. If $\nu \subseteq \text{supp}(sb_t)$ and $\psi(\nu) = \sigma$, then $\nu \subseteq \text{supp}(s)$ so $\phi_\sigma(sb_t) = \phi_\sigma(s)$ and thus $\delta_\sigma(sb_t) = \delta_\sigma(s)$.

Now assume that $a_k = i$. In this case $\phi_\sigma(sb_t) = \phi_\sigma(s) \cup \{\nu \cup \{t\} : \nu \in \phi_{\sigma'}(s)\}$ so $\delta_\sigma(sb_t) = \delta_\sigma(s) + \delta_{\sigma'}(s)$.

For the final conclusion note that for any $s \in S$, $\phi_\emptyset(s) = \{\emptyset\}$. □

4.10 Lemma. *Let $i \in \{1, 2, \ldots, n\}$, let r be an idempotent in V, let $z \in \beta S$ such that $zx_i r = r$, and let $\sigma = \langle a_1, a_2, \ldots, a_k \rangle \in E \setminus \{\emptyset\}$. Then $\widetilde{\delta}_\sigma(z) = 0$ unless $a_1 = a_2 = \ldots = a_k = i$, in which case $\widetilde{\delta}_\sigma(z) = (-1)^k$.*

Proof. First note that, by Lemma 4.8, $0 = \widetilde{\delta}_\sigma(r) = \widetilde{\delta}_\sigma(zx_ir) = \widetilde{\delta}_\sigma(zx_i)$.

We proceed by induction on k. If $k = 1$, then by Lemma 4.9,

$$\widetilde{\delta}_\sigma(zx_i) = \begin{cases} \widetilde{\delta}_\sigma(z) & \text{if } i \neq a_1 \\ \widetilde{\delta}_\sigma(z) + 1 & \text{if } i = a_1 \end{cases} \quad \text{so} \quad \widetilde{\delta}_\sigma(z) = \begin{cases} 0 & \text{if } i \neq a_1 \\ -1 & \text{if } i = a_1. \end{cases}$$

Now let $k > 1$ and assume the result holds for $k - 1$. Let $\sigma' = \langle a_1, a_2, \ldots, a_{k-1} \rangle$. By Lemma 4.9,

$$\widetilde{\delta}_\sigma(zx_i) = \begin{cases} \widetilde{\delta}_\sigma(z) & \text{if } i \neq a_1 \\ \widetilde{\delta}_\sigma(z) + \widetilde{\delta}_{\sigma'}(z) & \text{if } i = a_1 \end{cases} \quad \text{so} \quad \widetilde{\delta}_\sigma(z) = \begin{cases} 0 & \text{if } i \neq a_1 \\ -\widetilde{\delta}_{\sigma'}(z) & \text{if } i = a_1. \end{cases}$$

Thus if $a_1 = a_2 = \ldots = a_k = i$, then $\widetilde{\delta}_\sigma(z) = (-1)^k$ and $\widetilde{\delta}_\sigma(z) = 0$ otherwise. □

Recall that we have fixed an idempotent $p \in K(V)$. Fix an idempotent $q \in K(C)$. For $i \in \{1, 2, \ldots, n\}$ let y_i be the inverse of px_ip in the group pVp and let z_i be the inverse of qx_iq in the group qCq.

4.11 Lemma. *Let $i \in \{1, 2, \ldots, n\}$ and let $l \in \{1, 2, \ldots, M - 1\}$.*

(a) $\widetilde{\delta}_{\langle i \rangle}\big((z_i)^l\big) = -l$ and $\widetilde{\delta}_{\langle i \rangle}\big((qx_iq)^l\big) = l$.

(b) Let $\sigma = \langle a_1, a_2, \ldots, a_k \rangle \in E \setminus \{\emptyset\}$ and assume that it is not the case that $a_1 = a_2 = \ldots = a_k = i$. Then $\widetilde{\delta}_\sigma\big((z_i)^l\big) = \widetilde{\delta}_\sigma\big((qx_iq)^l\big) = 0$.

Proof. By Lemma 4.5, $\widetilde{\delta}_{\langle i \rangle}$ is a homomorphism and hence $\widetilde{\delta}_{\langle i \rangle}(q) = 0$. So (a) follows immediately from the observation that $\widetilde{\delta}_{\langle i \rangle}(x_i) = 1$.

We establish (b) by induction on k. If $k = 1$, then $a_1 \neq 1$ so by Lemma 4.9 $\widetilde{\delta}_\sigma\big((z_i)^l\big) = \widetilde{\delta}_\sigma\big((z_i)^l x_i\big) = \widetilde{\delta}_\sigma\big((z_i)^{l-1}\big) = 0$ and $\widetilde{\delta}_\sigma\big((qx_iq)^l\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}x_iq\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}x_i\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}\big) = 0$. Now assume that $k > 1$ and (b) holds for $k - 1$. If $a_k \neq i$, then exactly as above $\widetilde{\delta}_\sigma\big((qx_iq)^l\big) = \widetilde{\delta}_\sigma\big((z_i)^l\big) = 0$, so assume that $a_k = i$ and let $\sigma' = \langle a_1, a_2, \ldots, a_{k-1} \rangle$. Then it is not the case that $a_1 = a_2 = \ldots = a_{k-1}$ so by Lemma 4.9, $0 = \widetilde{\delta}_\sigma\big((z_i)^{l-1}\big) = \widetilde{\delta}_\sigma\big((z_i)^l x_i\big) = \widetilde{\delta}_\sigma\big((z_i)^l\big) + \widetilde{\delta}_{\sigma'}\big((z_i)^l\big) = \widetilde{\delta}_\sigma\big((z_i)^l\big)$. Also $\widetilde{\delta}_\sigma\big((qx_iq)^l\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}x_iq\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}x_i\big) = \widetilde{\delta}_\sigma\big((qx_iq)^{l-1}\big) + \widetilde{\delta}_{\sigma'}\big((qx_iq)^{l-1}\big) = 0$. □

4.12 Definition. For $v, v' \in \beta S$, $v \sim v'$ if and only if for all $\sigma \in E \setminus \{\emptyset\}$, $\widetilde{\delta}_\sigma(v) = \widetilde{\delta}_\sigma(v')$.

4.13 Lemma. *Let $v, v' \in \beta S$ and assume that $v \sim v'$.*

(a) If r, r' are idempotents in V, then $vr \sim v'r'$.

(b) For every $i \in \{1, 2, \ldots, n\}$, $vx_i \sim v'x_i$ and $vy_i \sim v'z_i$.

Proof. (a) By Lemma 4.8, $\widetilde{\delta}_\sigma(vr) = \widetilde{\delta}_\sigma(v) = \widetilde{\delta}_\sigma(v') = \widetilde{\delta}_\sigma(v'r')$.

(b) We have $vy_ix_ip = vp$ and $v'z_ix_iq = v'q$ so by Lemma 4.8 for any $\sigma \in E \setminus \{\emptyset\}$, $\widetilde{\delta}_\sigma(vy_ix_i) = \widetilde{\delta}_\sigma(vy_ix_ip) = \widetilde{\delta}_\sigma(vp) = \widetilde{\delta}_\sigma(v) = \widetilde{\delta}_\sigma(v') = \widetilde{\delta}_\sigma(v'q) = \widetilde{\delta}_\sigma(v'z_ix_iq) = \widetilde{\delta}_\sigma(v'z_ix_i)$, so $vy_ix_i \sim v'z_ix_i$.

We now proceed by induction on the length of σ. Assume first that $\sigma = \langle a_1 \rangle$. Then by Lemma 4.9 either

(1) $\widetilde{\delta}_\sigma(vy_ix_i) = \widetilde{\delta}_\sigma(vy_i)$, $\widetilde{\delta}_\sigma(v'z_ix_i) = \widetilde{\delta}_\sigma(v'z_i)$, $\widetilde{\delta}_\sigma(vx_i) = \widetilde{\delta}_\sigma(v)$, and $\widetilde{\delta}_\sigma(v'x_i) = \widetilde{\delta}_\sigma(v')$; or

(2) $\widetilde{\delta}_\sigma(vy_ix_i) = \widetilde{\delta}_\sigma(vy_i) + 1$, $\widetilde{\delta}_\sigma(v'z_ix_i) = \widetilde{\delta}_\sigma(v'z_i) + 1$, $\widetilde{\delta}_\sigma(vx_i) = \widetilde{\delta}_\sigma(v) + 1$, and $\widetilde{\delta}_\sigma(v'x_i) = \widetilde{\delta}_\sigma(v') + 1$.

In either case $\widetilde{\delta}_\sigma(vy_i) = \widetilde{\delta}_\sigma(v'z_i)$ and $\widetilde{\delta}_\sigma(vx_i) = \widetilde{\delta}_\sigma(v'x_i)$.

Now assume that $k > 1$, $\sigma' = \langle a_1, a_2, \ldots, a_{k-1} \rangle$, $\widetilde{\delta}_{\sigma'}(vy_i) = \widetilde{\delta}_{\sigma'}(v'z_i)$, and $\widetilde{\delta}_{\sigma'}(vx_i) = \widetilde{\delta}_{\sigma'}(v'x_i)$. Again applying Lemma 4.9 we see that $\widetilde{\delta}_\sigma(vy_i) = \widetilde{\delta}_\sigma(v'z_i)$, and $\widetilde{\delta}_\sigma(vx_i) = \widetilde{\delta}_\sigma(v'x_i)$. □

4.14 Lemma. *Let $m \in \mathbb{N}$ and let $j_1, j_2, \ldots, j_m \in \{1, 2, \ldots, n\}$. Assume that for each $i \in \{1, 2, \ldots, m\}$, either $v_i = px_{j_i}p$ and $v'_i = qx_{j_i}q$ or $v_i = y_{j_i}$ and $v'_i = z_{j_i}$. Let $u = v_1 \cdot v_2 \cdots v_m$ and let $u' = v'_1 \cdot v'_2 \cdots v'_m$. Then $u \sim u'$.*

Proof. Note that by Lemma 4.8, $p \sim q$. We proceed by induction on m. If $m = 1$, the result is an immediate consequence of Lemma 4.13 (noting that $py_i = y_i$ and $qz_i = z_i$).

Now assume that $m > 1$ and $v_1 \cdot v_2 \cdots v_{m-1} \sim v'_1 \cdot v'_2 \cdots v'_{m-1}$. Then applying Lemma 4.13 twice we have $v_1 \cdot v_2 \cdots v_{m-1} \cdot p \sim v'_1 \cdot v'_2 \cdots v'_{m-1} \cdot q$ so $v_1 \cdot v_2 \cdots v_m \sim v'_1 \cdot v'_2 \cdots v'_m$. □

We are now ready to conclude the proof of Theorem 4.4. Recall that we have assumed that we have $d \in \mathbb{N}$, $w_1, w_2, \ldots, w_d \in pVp$, $l_1, l_2, \ldots, l_d \in \mathbb{N}$, and $j_1, j_2, \ldots, j_d \in \{1, 2, \ldots, n\}$ such that $(w_1)^{l_1} \cdot (w_2)^{l_2} \cdots (w_d)^{l_d} = p$, for each $i \in \{1, 2, \ldots, d\}$, either $w_i = px_{j_i}p$ or $w_i = y_{j_i}$, and if $i \in \{1, 2, \ldots, d-1\}$, then $j_i \neq j_{i-1}$. (All of these things were introduced at the start of the proof of Theorem 4.4 except for $j_1, j_2, \ldots, j_d$. These can be determined from the fact that $\{x_1, x_2, \ldots, x_n\} = \{r_{t(i)} : i \in \{1, 2, \ldots, d\}\}$.)

Let $\sigma = \langle j_1, j_2, \ldots, j_d \rangle$ and let $u = (w_1)^{l_1} \cdot (w_2)^{l_2} \cdots (w_d)^{l_d}$. We shall show that $\widetilde{\delta}_\sigma(u) \neq 0$, which will be a contradiction since $\widetilde{\delta}_\sigma(p) = 0$.

For $i \in \{1, 2, \ldots, d\}$, let $w'_i = qx_{j_i}q$ if $w_i = px_{j_i}p$ and let $w'_i = z_{j_i}$ if $w_i = y_{j_i}$. Let $u' = (w'_1)^{l_1} \cdot (w'_2)^{l_2} \cdots (w'_d)^{l_d}$. By Lemma 4.14, $u \sim u'$ so it suffices to show that

$\widetilde{\delta}_\sigma(u') \neq 0$.

Let $E' = \{\tau \in E : \text{the length of } \tau \text{ is less than } d\}$. For $m \in \{1, 2, \ldots, d\}$, let

$$A_m = \Big\{ s_1 \cdot s_2 \cdots s_m : (\forall i \in \{1, 2, \ldots, m-1\})(\max \operatorname{supp}(s_i) < \min \operatorname{supp}(s_{i+1})) \text{ and } (\forall \tau \in E')(\forall i \in \{1, 2, \ldots, m\}) \left(\delta_\tau(s_i) = \widetilde{\delta}_\tau\big((w_i')^{l_i}\big) \right) \Big\}.$$

We show by induction on m that $A_m \in (w_1')^{l_1} \cdot (w_2')^{l_2} \cdots (w_m')^{l_m}$. For each $\tau \in E'$ pick $R_\tau \in (w_1')^{l_1}$ such that for all $s \in R_\tau$, $\delta_\tau(s) = \widetilde{\delta}_\tau\big((w_1')^{l_1}\big)$. Then $\bigcap_{\tau \in E'} R_\tau \subseteq A_1$ so $A_1 \in (w_1')^{l_1}$.

Now let $m \in \{1, 2, \ldots, d-1\}$ and assume that $A_m \in (w_1')^{l_1} \cdot (w_2')^{l_2} \cdots (w_m')^{l_m}$. We show that

$$A_m \subseteq \{t \in S : t^{-1} A_{m+1} \in (w_{m+1}')^{l_{m+1}}\}$$

so that $A_{m+1} \in (w_1')^{l_1} \cdot (w_2')^{l_2} \cdots (w_{m+1}')^{l_{m+1}}$ as required. Let $t \in A_m$ and pick $s_1, s_2, \ldots, s_m$ as in the definition of A_m so that $t = s_1 \cdot s_2 \cdots s_m$. For each $\tau \in E'$ pick $R_\tau \in (w_{m+1}')^{l_{m+1}}$ such that for all $s \in R_\tau$, $\delta_\tau(s) = \widetilde{\delta}_\tau\big((w_{m+1}')^{l_{m+1}}\big)$. Let $T = \{v \in S : \min \operatorname{supp}(v) > \max \operatorname{supp}(s_m)\}$. Then since $(w_{m+1}')^{l_{m+1}} \in C$, we have $T \in (w_{m+1}')^{l_{m+1}}$. (This fact is the reason for working with u' rather than u.) Then $T \cap \big(\bigcap_{\tau \in E'} R_\tau\big) \subseteq t^{-1} A_{m+1}$ so $t^{-1} A_{m+1} \in (w_{m+1}')^{l_{m+1}}$ as required.

We thus have that $A_d \in u'$. We also know that $\{t \in S : \delta_\sigma(t) = \widetilde{\delta}_\sigma(u')\} \in u'$. We shall show that for $t \in A$ such that $\delta_\sigma(t) = \widetilde{\delta}_\sigma(u')$, either $\delta_\sigma(t) = \prod_{i=1}^d l_i$ or $\delta_\sigma(t) = -\prod_{i=1}^d l_i$. Recalling that $M = 1 + \prod_{i=1}^d l_i$, we will then have that $\widetilde{\delta}_\sigma(u') \neq 0$. To this end let $t \in A_d$ and pick $s_1, s_2, \ldots, s_d$ such that $t = s_1 \cdot s_2 \cdots s_d$, for all $i \in \{1, 2, \ldots, m-1\}$, $\max \operatorname{supp}(s_i) < \min \operatorname{supp}(s_{i+1})$, and for all $\tau \in E'$ and all $i \in \{1, 2, \ldots, m\}$, $\delta_\tau(s_i) = \widetilde{\delta}_\tau\big((w_i')^{l_i}\big)$.

Let $H = \{(\rho_1, \rho_2, \ldots, \rho_d) \in E^d : \sigma = \rho_1 \frown \rho_2 \frown \ldots \frown \rho_d\}$ (where $\frown$ denotes concatenation) and for $(\rho_1, \rho_2, \ldots, \rho_d) \in H$, let

$$G_{(\rho_1, \rho_2, \ldots, \rho_d)} = \{\mu \in \phi_\sigma(t) : (\forall i \in \{1, 2, \ldots, d\})(\psi\big(\mu \cap \operatorname{supp}(s_i)\big) = \rho_i)\}.$$

We note that $|G_{(\rho_1, \rho_2, \ldots, \rho_d)}| = \prod_{i=1}^d |\phi_{\rho_i}(s_i)|$ because there are precisely $|\phi_{\rho_i}(s_i)|$ choices for $\mu \cap \operatorname{supp}(s_i)$ with $\psi\big(\mu \cap \operatorname{supp}(s_i)\big) = \rho_i$. Note also that

$$\phi_\sigma(t) = \bigcup_{(\rho_1, \rho_2, \ldots, \rho_d) \in H} G_{(\rho_1, \rho_2, \ldots, \rho_d)}$$

and these sets are pairwise disjoint so $|\phi_\sigma(t)| = \sum_{(\rho_1, \rho_2, \ldots, \rho_d) \in H} \prod_{i=1}^d |\phi_{\rho_i}(s_i)|$.

Now, if $(\rho_1, \rho_2, \ldots, \rho_d) \in H$ and $(\rho_1, \rho_2, \ldots, \rho_d) \neq (\langle j_1 \rangle, \langle j_2 \rangle, \ldots, \langle j_d \rangle)$, then for some $i \in \{1, 2, \ldots, d\}$, ρ_i is neither empty nor constant so, by Lemma 4.11, $\delta_{\rho_i}(s_i) = \widetilde{\delta}_{\rho_i}\big((w_i')^{l_i}\big) = 0$ and thus $|\phi_{\rho_i}(s_i)| \equiv 0 \pmod{M}$. Consequently $\widetilde{\delta}_\sigma(u') = \delta_\sigma(t) \equiv$

$|\phi_\sigma(t)| \pmod M \equiv \prod_{i=1}^d |\phi_{\langle j_i\rangle}(s_i)| \pmod M$. By Lemma 4.11 for $i \in \{1, 2, \ldots, d\}$, $|\phi_{\langle j_i\rangle}(s_i)| \equiv \delta_{\langle j_i\rangle}(s_i) \pmod M \equiv \widetilde{\delta}_{\langle j_i\rangle}\big((w_i)^{l_i}\big) = \pm l_i$ and thus either $\delta_\sigma(t) = \prod_{i=1}^d l_i$ or $\delta_\sigma(t) = -\prod_{i=1}^d l_i$. □

We show now that if S is left cancellative, then Theorem 4.4 yields a result about the smallest ideal of βS.

4.15 Theorem. *If S is left cancellative, then $V \cap K(\beta S) \neq \emptyset$ and so $K(V) = K(\beta S) \cap V$.*

Proof. We show that given any minimal left ideal L of βS, $V \cap L \neq \emptyset$. It suffices to show that for each $J \in \mathcal{P}_f(\kappa)$, $L \cap \overline{D}_J \neq \emptyset$ because then $\{L \cap c\ell_{\beta S} D_J : J \in \mathcal{P}_f(\kappa)\}$ is a collection of closed subsets of βS with the finite intersection property, and therefore has nonempty intersection.

So let $J \in \mathcal{P}_f(\kappa)$. We observe that every $s \in S$ can be written uniquely as $s = ab$ where $a \in S$ satisfies $\mathrm{supp}(a) \subseteq J$ and $b \in D_J$, and that $\{a \in S : \mathrm{supp}(a) \subseteq J\}$ is finite. Hence, if p is an idempotent in L, then $p = ax$ for some $a \in S$ and some $x \in \overline{D}_J$. Now $axp = ax$ and this implies that $x = xp$ by [9, Lemma 8.1]. So $x \in L$ and and thus $L \cap \overline{D}_J \neq \emptyset$.

The fact that $K(V) = K(\beta S) \cap V$ follows from [9, Theorem 1.65]. □

Recall that we are assuming that S is an infinite semigroup, that $|S| = \kappa$ and that S has a digital representation with the property that $ab = ba$ whenever $a, b \in S$ satisfy $a \perp b$.

4.16 Corollary. *If S is left cancellative, then the structure group of S contains a copy of the free group on 2^{2^κ} generators.*

Proof. Pick an idempotent $p \in K(V)$. Then, by Theorem 4.15, $pVp \subseteq K(\beta S)$ and so Theorem 4.4 applies. □

We now show that Corollary 4.16 can be extended to many semigroups which may not satisfy the hypotheses used in the proof of this corollary.

4.17 Theorem. *Let T be a discrete semigroup and assume that there is a discrete semigroup S whose structure group contains a copy of the free group on 2^{2^κ} generators and that there is a homomorphism $h : T \xrightarrow{\text{onto}} S$. Then the structure group of βT contains a copy of the free group on 2^{2^κ} generators.*

Proof. Let $\widetilde{h} : \beta T \to \beta S$ be the continuous extension of h. Then by [9, Corollary 4.22] $\widetilde{h}$ is a homomorphism and $\widetilde{h}[\beta T] = \beta S$ by [9, Exercise 3.4.1] so by [9, Exercise 1.7.3] $K(\beta S) = \widetilde{h}[K(\beta T)]$. Let p be an idempotent in $K(\beta S)$ and let G be a copy of the free group on 2^{2^κ} generators contained in $p\beta Sp$ (which exists by assumption). Then $\widetilde{h}^{-1}[\{p\}] \cap K(T) \neq \emptyset$ so pick a minimal left ideal L of βT such that $\widetilde{h}^{-1}[\{p\}] \cap L \neq \emptyset$. Then $\widetilde{h}^{-1}[\{p\}] \cap L$ is a compact subsemigroup of βT so pick an idempotent $q \in \widetilde{h}^{-1}[\{p\}] \cap L$. Then $\widetilde{h}[q\beta Tq] = p\beta Sp$. Let A be the set of generators of G and for $a \in A$, pick $f(a) \in q\beta Tq$ such that $\widetilde{h}\big(f(a)\big) = a$. Then since G is a free group, f extends to a homomorphism $f^* : G \to q\beta Tq$. For any $w \in G$, $\widetilde{h}\big(f^*(w)\big) = w$ so f^* is injective. □

4.18 Corollary. *Let $\kappa \geq \omega$ and let T be either the free semigroup with identity or the free group on the generators $\langle a_\lambda \rangle_{\lambda<\kappa}$. Then the structure group of βT contains a copy of the free group on 2^{2^κ} generators.*

Proof. If T is the free semigroup with identity on the generators $\langle a_\lambda \rangle_{\lambda<\kappa}$, let $S = \bigoplus_{\lambda<\kappa}(\omega, +)$. If T is the free group, let $S = \bigoplus_{\lambda<\kappa}(\mathbb{Z}, +)$. In either case S is cancellative and commutative and by Theorem 1.1, S has a digital representation. By Corollary 4.16 the structure group of S contains a copy of the free group on 2^{2^κ} generators. Given $\lambda < \kappa$, let $h(a_\lambda) \in S$ be defined by, for $\tau < \lambda$,

$$h(a_\lambda)(\tau) = \begin{cases} 1 & \text{if } \tau = \lambda \\ 0 & \text{if } \tau \neq \lambda\,. \end{cases}$$

Extend h to a homomorphism on T and note that h is surjective, so that Theorem 4.17 applies. □

We now give an application of digital representations to weakly almost periodic compactifications. In the sequel S will denote an infinite discrete abelian group with cardinality κ, WAP(S) will denote the algebra of weakly almost periodic functions defined on S and S^{WAP} will denote the weakly almost periodic compactification of S. The mapping $\pi : \beta S \to S^{WAP}$ will denote the canonical homomorphism. We observe that, for any $x, y \in \beta S$, $\pi(x) = \pi(y)$ if and only if $\widetilde{f}(x) = \widetilde{f}(y)$ for every $f \in \mathrm{WAP}(S)$, where $\widetilde{f}$ denotes the continuous extension of f to βS. We remind the reader that S^{WAP} is a commutative semigroup.

By Theorem 3.9, S has a digital representation $\langle F_t \rangle_{t\in\kappa}$. For $s \in S$, we define supp(s) and V as in Definition 4.2. We define $\alpha : S \to \omega$ by $\alpha(s) = |\mathrm{supp}(s)|$. Then $\widetilde{\alpha} : \beta S \to \beta\omega$ will denote the continuous extension of α. For any subset J of κ and any $s \in S$, we put $\alpha_J(s) = |J \cap \mathrm{supp}(s)|$ and use $\widetilde{\alpha}_J : \beta S \to \beta\omega$ for the continuous extension of α_J. (So the mapping γ_J introduced above, is α_J reduced modulo M.)

4.19 Lemma. *Let S be an abelian group with cardinality κ. Given $n \in \mathbb{N}$, put $A_n = \{s \in S : \alpha(s) \leq n\}$. Then $\chi_{A_n} \in \mathrm{WAP}(S)$. Furthermore, for every $J \subseteq \kappa$, $\chi_{A_n} \cdot \alpha_J \in \mathrm{WAP}(S)$.*

Proof. By [9, Theorem 21.18], to see that $\chi_{A_n} \in \mathrm{WAP}(S)$, it is sufficient to show that $\widetilde{\chi}_{A_n}(xy) = \widetilde{\chi}_{A_n}(yx)$ for every $x, y \in \beta S$.

We first show that every $z \in \overline{A}_n$ can be written as $z = cw$, where $c \in S$, $w \in V$ and $\widetilde{\alpha}(w) \in \omega$. To see this, put $S_t = \{s \in S : t \in \mathrm{supp}(s)\}$ for each $t \in \kappa$, and put $H = \{t \in \kappa : S_t \in z\}$. We claim that H is a finite set with cardinality at most n. To see this, let H' denote any finite subset of H. Then $\bigcap_{t\in H'} S_t \subseteq \{s \in S : \alpha(s) \geq |H'|\}$. Since $\bigcap_{t\in H'} S_t \in z$, it follows that $|H'| \leq n$. Given $s \in S$, write $s = \prod_{t\in \mathrm{supp}(s)} x_t$ with each $x_t \in F_t$ and put $f(s) = \prod_{t\in \mathrm{supp}(s)\cap H} x_t$. Then, $S = \bigcup\{f^{-1}[\{c\}] : c \in S$ and $\mathrm{supp}(c) \subseteq H\}$. Since $\{c \in S : \mathrm{supp}(c) \subseteq H\}$ is finite, for some $c \in S$ with $\mathrm{supp}(c) \subseteq H$, we have $f^{-1}[\{c\}] \in z$.

We claim that or each $F \in \mathcal{P}_f(\kappa)$ such that $F \cap H = \emptyset$, $c^{-1}z \in \overline{D}_{H\cup F}$, so let such F be given and let $L = \bigcap_{t\in F}(S \setminus S_t)$ Then $L \in z$ and therefore $c^{-1}(L \cap f^{-1}[\{c\}]) \in c^{-1}z$. We claim that $c^{-1}(L \cap f^{-1}[\{c\}]) \subseteq \overline{D}_{H\cup F}$, so let $y \in c^{-1}(L \cap f^{-1}[\{c\}])$. Then $cy = \prod_{t\in \mathrm{supp}(cy)} x_t$ where each $x_t \in F_t$ and $c = f(cy) = \prod_{t\in \mathrm{supp}(cy)\cap H} x_t$. Thus $y = \prod_{t\in \mathrm{supp}(cy)\setminus H} x_t$ and in particular, $\mathrm{supp}(y) = \mathrm{supp}(cy)\setminus H$. Suppose that $y \notin D_{H\cup F}$ and pick $t \in \mathrm{supp}(y) \cap (H \cup F)$. Then $t \in (\mathrm{supp}(cy) \setminus H) \cap F$. But $cy \in L \subseteq S \setminus S_t$ so $t \notin \mathrm{supp}(cy)$, a contradiction. As a consequence we have that $c^{-1}z \in V$ and hence that $z = cw$ for some $w \in V$. By Lemma 4.5, this implies that $\alpha(c)\widetilde{\alpha}(w) = \widetilde{\alpha}(z) \in \omega$. So $\widetilde{\alpha}(w) \in \omega$, because $\beta\omega \setminus \omega$ is an ideal of $\beta\omega$ [9, Theorem 4.36].

Now assume that $xy \in \overline{A}_n$. Then there exists $s \in S$ such that $sy \in \overline{A}_n$. Thus there exist $c \in S$ and $v \in V$ such that $sy = cv$ and $\widetilde{\alpha}(v) \in \omega$. Let $b = s^{-1}c$. Then $y = bv$. Then, using the fact that S is contained in the center of βS, $xy = bxv \in \overline{A}_n$. By Lemma 4.5, $\widetilde{\alpha}(xy) = \widetilde{\alpha}(bx)\widetilde{\alpha}(v) \in \omega$, and hence $\widetilde{\alpha}(bx) \in \omega$. Consequently, $bx \in A_m$ for some $m \in \omega$ so we also have $x = au$ for some $a \in S$ and some $u \in V$ satisfying $\widetilde{\alpha}(u) \in \omega$. So $\widetilde{\alpha}(xy) = \widetilde{\alpha}(ab)\widetilde{\alpha}(u)\widetilde{\alpha}(v) = \widetilde{\alpha}(ab)\widetilde{\alpha}(v)\widetilde{\alpha}(u) = \widetilde{\alpha}(yx)$. So $\widetilde{\chi}_{A_n}(xy) = \widetilde{\chi}_{A_n}(yx)$, and $\chi_{A_n} \in \mathrm{WAP}(S)$, as claimed.

Similarly, it follows from Lemma 4.5 that, if $xy \in \overline{A}_n$ for some $n \in \omega$, then $\widetilde{\alpha}_J(xy) = \widetilde{\alpha}_J(yx)$. So $\chi_{A_n} \cdot \alpha_J \in \mathrm{WAP}(S)$. □

4.20 Theorem. *Copies of the free abelian semigroup on 2^{2^κ} generators exist in S^{WAP}.*

Proof. As in the proof of Theorem 4.4, we choose $b_t \in F_t$ for each $t < \kappa$, and use U to denote the set of uniform ultrafilters on $\{b_t : t < \kappa\}$. We note that $|U| = 2^{2^\kappa}$.

We choose a finite number of distinct elements $x_1, x_2, \ldots, x_n$ in U and a partition of κ into disjoint subsets $J_1, J_2, \ldots, J_n$ with the property that $\{b_t : t \in J_i\} \in x_i$ for each $i \in \{1, 2, \ldots, n\}$.

Suppose that $u = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$ and that $v = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$, where $k_i, m_i \in \omega$ and $\langle k_1, k_2, \ldots, k_n \rangle \neq \langle m_1, m_2, \ldots, m_n \rangle$. We shall show that $\pi(u) \neq \pi(v)$. It will follow that $\pi[U]$ generates a free abelian subsemigroup of S^{WAP}.

To see this, choose $N > \sum_{i=1}^n (k_i + m_i)$. It is easy to verify that $\widetilde{\alpha}(u) = \sum_{i=1}^n k_i$ and $\widetilde{\alpha}(v) = \sum_{i=1}^n m_i$, so that $u, v \in \overline{A}_N$. Now $\widetilde{\alpha}_{J_i}(x_j) = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$. By Lemma 4.5, $\widetilde{\alpha}_{J_i}$ is a homomorphism on V. So $\widetilde{\alpha}_{J_i}(u) = k_i$ and $\widetilde{\alpha}_{J_i}(v) = m_i$ for each $i \in \{1, 2, \ldots, n\}$. We can choose $i \in \{1, 2, \ldots, n\}$ for which $k_i \neq m_i$. Then $\widetilde{\chi}_{A_N} \cdot \widetilde{\alpha}_{J_i}(u) \neq \widetilde{\chi}_{A_N} \cdot \widetilde{\alpha}_{J_i}(v)$. By Lemma 4.19, $\chi_{A_N} \cdot \alpha_{J_i} \in \mathrm{WAP}(S)$ and so $\pi(u) \neq \pi(v)$. □

Theorem 4.20 illustrates the fact that the existence of free algebraic structures in a compact right topological semigroup T, can be very different from their existence in $K(T)$. For example, suppose that S is a direct sum of copies of $\mathbb{Z}_2$. It is well-known that $K(S^{WAP})$ is the Bohr compactification of S and that this is a group with index 2. So $K(S^{WAP})$ contains no non-trivial free abelian semigroups.

References

[1] B. Bordbar and J. Pym, *The set of idempotents in the weakly almost periodic compactification of the integers is not closed*, Trans. Amer. Math. Soc. **352** (2000), 823–842.

[2] T. Budak, N. Işik, and J. Pym, *Subsemigroups of Stone-Čech compactifications*, Math. Proc. Cambr. Phil. Soc. **116** (1994), 99–118.

[3] H. G. Dales, A. Lau and D. Strauss, Banach algebras on semigroups and their compactifications, manuscript*.

[4] C. F. Gauss, *Analysis residuorum: Caput octavum*, Disquisitiones generales de congruentiis, Königlichen Gesellschaft der Wissenschaften, Gottingen, 1876; Untersuchungen über Höhere Arithmetik (H. Maser, ed.), Springer, Berlin, 1889, 602–629. Available on line:
`http://www-gdz.sub.uni-goettingen.de/cgi-bin/digbib.cgi?PPN23599524X`

[5] D. Gorenstein, R. Lyons, and R. Solomon, *The classification of the finite simple groups*, American Mathematical Society, Providence, 1994.

* Currently available at `http://www.maths.leeds.ac.uk/~pmt6hgd/`.

[6] E. Hewitt and K. Ross, *Abstract Harmonic Analysis, I*, Springer-Verlag, Berlin, 1963.

[7] N. Hindman, I. Leader, and D. Strauss, *Separating Milliken-Taylor systems with negative entries*, Proc. Edinburgh Math. Soc. **46** (2003), 45–61.

[8] N. Hindman and J. Pym, *Free groups and semigroups in $\beta\mathbb{N}$*, Semigroup Forum **30** (1984), 177–193.

[9] N. Hindman and D. Strauss, *Algebra in the Stone-Čech compactification: theory and applications*, de Gruyter, Berlin, 1998.

[10] N. Hindman and D. Strauss, *Bases for commutative semigroups and groups*, Math. Proc. Cambr. Phil. Soc., to appear**.

[11] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[12] D. Madore, *Orders of nonabelian simple groups.* `http://www.madore.org/~david/math/simplegroups.html`

[13] J. Pym, *Semigroup structure in Stone-Čech compactifications*, J. London Math. Soc. **36** (1987), 421-428.

[14] W. Ruppert, *On signed* **a**-*adic expansions and weakly almost periodic functions*, Proc. London Math. Soc. **63** (1991), 620–656.

Stefano Ferri
Departamento de Matemáticas
Universidad de los Andes
Carrera 1 n.o 18A-10
Bogotá
Apartado Aéreo 4976
Colombia
`stferri@uniandes.edu.co`

Neil Hindman
Department of Mathematics
Howard University
Washington, DC 20059
USA
`nhindman@aol.com`

Dona Strauss
Mathematics Centre
University of Hull
Hull HU6 7RX
UK
`d.strauss@hull.ac.uk`

** Currently available at `http://members.aol.com/nhindman/`.