This paper was published in *Topology and its Applications*, **154** (2007), 2099-2103. To the best of my knowledge, this is the final version as it was submitted to the publisher. –NH

Discrete Groups in $\beta\mathbb{N}$

Neil Hindman[1]

and

Dona Strauss

Abstract. We show that every maximal group in the smallest ideal of $(\beta\mathbb{N}, +)$ contains $2^{\mathfrak{c}}$ discrete copies of $(\mathbb{Z}, +)$ the closures of any two of which intersect only at the identity. We also show that the same conclusion applies to copies of the free group on two generators (and consequently the free group on countably many generators).

1. Introduction

Of course topological copies of $\mathbb{Z}$ (i.e., countably infinite discrete sets) are plentiful in the Stone-Čech compactification $\beta\mathbb{N}$ of the set $\mathbb{N}$ of positive integers. And algebraic copies of $(\mathbb{Z}, +)$ are also easy to come by; given any idempotent $p = p+p$ in $\beta\mathbb{N}$, $\{n+p : n \in \mathbb{Z}\}$ is an algebraic copy of $\mathbb{Z}$. However, a subgroup of $\mathbb{N}^*$ of this kind cannot be discrete. Further, discrete algebraic copies of $\mathbb{N}$ are plentiful. If for example $p \in c\ell\{2^n : n \in \mathbb{N}\}$, then $\{p, p+p, p+p+p, \ldots\}$ is discrete.

We show in this paper that discrete algebraic copies of $\mathbb{Z}$ as well as the discrete free semigroup on two generators are also plentiful.

Let us begin with a brief review of the algebraic structure of $(\beta\mathbb{N}, +)$. We view $\beta\mathbb{N}$ as the set of ultrafilters on $\mathbb{N}$, identifying the points of $\mathbb{N}$ with the principal ultrafilters. The operation $+$ extends to $\beta\mathbb{N}$ making $(\beta\mathbb{N}, +)$ a compact right topological semigroup (meaning that for each $p \in \beta\mathbb{N}$, the function ρ_p defined by $\rho_p(q) = q + p$ is continuous) with $\mathbb{N}$ contained in its topological center (meaning that for each $x \in \mathbb{N}$, the function λ_x defined by $\lambda_x(q) = x + q$ is continuous). As with any compact (Hausdorff) right topological semigroup, $(\beta\mathbb{N}, +)$ has a smallest two sided ideal $K(\beta\mathbb{N})$. This ideal is the union of all of the minimal right ideals as well as the union of all of the minimal left ideals. The intersection of any minimal left ideal with any minimal right ideal is a group, and any two such groups are isomorphic. In $\beta\mathbb{N}$ there are $2^{\mathfrak{c}}$ minimal right ideals and

[1]This author acknowledges support received from the National Science Foundation (USA) via grants DMS 0243586 and DMS 0554803.

$2^{\mathfrak{c}}$ minimal left ideals, and consequently $2^{\mathfrak{c}}$ maximal groups in the smallest ideal. Given p and q in $\beta\mathbb{N}$ and $A \subseteq \mathbb{N}$, $A \in p+q$ if and only if $\{x \in \mathbb{N} : -x+A \in q\} \in p$, where $-x+A = \{y \in \mathbb{N} : x+y \in A\}$. See [1] for more details and any unfamiliar algebraic facts encountered in this paper.

Any idempotent p of $\beta\mathbb{N}$, whether in the smallest ideal or not, is the identity of a maximal group $H(p)$. It is consistent that this maximal group is as small as possible, namely $\{n+p : n \in \mathbb{Z}\}$, which is an algebraic copy of $\mathbb{Z}$ [1, Theorem 12.42]. Notice that such a copy cannot be discrete because $p = p+p \in c\ell\{n+p : n \in \mathbb{N}\}$. The maximal groups in the smallest ideal are all as large as possible; they each contain a copy of the free group on $2^{\mathfrak{c}}$ generators ([2], or see [1, Corollary 7.37]). It is a result of Y. Zelenyuk [4] that there are no nontrivial finite groups in $\beta\mathbb{N}$.

In Section 2 we show that there are $2^{\mathfrak{c}}$ discrete copies of $\mathbb{Z}$ in each of the maximal groups in the smallest ideal, and that any two of these meet only in the identity. In Section 3 we show that the same statement holds for the free group on 2 generators. Since the free group on 2 generators contains copies of $\mathbb{Z}$, the results of Section 2 are a corollary of those of Section 3. We present them separately because the proof for $\mathbb{Z}$ is simpler and the conclusion for $\mathbb{Z}$ is of independent interest.

2. Copies of $\mathbb{Z}$

We write $\mathbb{N}^*$ for $\beta\mathbb{N}\setminus\mathbb{N}$ and denote the set of finite nonempty subsets of a set X by $\mathcal{P}_f(X)$. Also $\omega = \mathbb{N} \cup \{0\}$. Given $x \in \mathbb{N}$, $\mathrm{supp}(x)$ is the $H \in \mathcal{P}_f(\omega)$ such that $x = \sum_{t\in H} 2^t$. We will have use for a particular subsemigroup of $\beta\mathbb{N}$, namely $\mathbb{H} = \bigcap_{n=1}^{\infty} \overline{2^n\mathbb{N}}$. By [1, Lemma 6.6] all idempotents of $(\beta\mathbb{N},+)$ lie in $\mathbb{H}$.

2.1 Theorem. *Let A and B be infinite disjoint subsets of $\mathbb{N}$. Let $q = q+q \in K(\beta\mathbb{N})$, let $u \in \mathbb{N}^* \cap c\ell\{2^n : n \in A\}$, and let $v \in \mathbb{N}^* \cap c\ell\{2^n : n \in B\}$. Let φ and ψ be the homomorphisms from $\mathbb{Z}$ into the group $q+\beta\mathbb{N}+q$ such that $\varphi(1) = q+u+q$ and $\psi(1) = q+v+q$. Then $c\ell\big\{\varphi(n) : n \in \mathbb{Z}\setminus\{0\}\big\} \cap c\ell\big\{\psi(n) : n \in \mathbb{Z}\setminus\{0\}\big\} = \emptyset$. If $q \notin c\ell\big\{\varphi(n) : n \in \mathbb{Z}\setminus\{0\}\big\}$, then $\{\varphi(n) : n \in \mathbb{Z}\}$ is a discrete copy of $\mathbb{Z}$. If $q \notin c\ell\big\{\psi(n) : n \in \mathbb{Z}\setminus\{0\}\big\}$, then $\{\psi(n) : n \in \mathbb{Z}\}$ is a discrete copy of $\mathbb{Z}$.*

Proof. Notice that $\psi[\mathbb{Z}] \cup \varphi[\mathbb{Z}] \subseteq \mathbb{H}$. We show first that for any $m \in \mathbb{Z}$ and any $n \in \mathbb{N}$,

$$\{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv 0 \pmod{n}\} \in \psi(m) \text{ and}$$
$$\{x \in \mathbb{N} : |\mathrm{supp}(x) \cap B| \equiv 0 \pmod{n}\} \in \varphi(m)\,.$$

It suffices to establish the former. Let $C = \{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv 0 \pmod{n}\}$. We show first that $C \in q$. Pick $i \in \{0,1,\ldots,n-1\}$ such that $D = \{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv$

$i \pmod n\} \in q$. Then $\{x \in \mathbb{N} : -x + D \in q\} \in q$ so pick $x \in D$ such that $-x + D \in q$. Let $t = \max \mathrm{supp}(x)$ and pick $y \in (-x + D) \cap D \cap 2^{t+1}\mathbb{N}$. Then $i \equiv |\mathrm{supp}(x + y) \cap A| = |\mathrm{supp}(x) \cap A| + |\mathrm{supp}(y) \cap A| \equiv i + i \pmod n$ so $i = 0$. That is $D = C$.

Now we show by induction on $m \in \omega$ that $C \in \psi(m)$. We have just shown that $C \in \psi(0)$. Assume that $m \in \omega$ and $C \in \psi(m)$. Now $\psi(m + 1) = \psi(m) + v + q$. To see that $C \in \psi(m) + v + q$, we show that $C \subseteq \{x \in \mathbb{N} : -x + C \in v + q\}$, so let $x \in C$. Let $t = \max \mathrm{supp}(x)$. We claim that $\{2^s : s \in B \text{ and } s > t\} \subseteq \{z \in \mathbb{N} : -z + (-x + C) \in q\}$. So let $s \in B$ with $s > t$. We claim that $C \cap 2^{s+1}\mathbb{N} \subseteq -2^s + (-x + C)$. So let $y \in C \cap 2^{s+1}\mathbb{N}$. Then since $s \notin A$, $|\mathrm{supp}(x + 2^s + y) \cap A| = |\mathrm{supp}(x) \cap A| + |\mathrm{supp}(y) \cap A| \equiv 0 \pmod n$.

To complete this portion of the proof, we let $m \in \mathbb{N}$ and show that $C \in \psi(-m)$. Pick $i \in \{0, 1, \ldots, n - 1\}$ such that $D = \{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv i \pmod n\} \in \psi(-m)$. Now $C \in q = \psi(-m) + \psi(m)$ so pick $x \in D$ such that $-x + C \in \psi(m)$. Let $t = \max \mathrm{supp}(x)$ and pick $y \in (-x + C) \cap C \cap 2^{t+1}\mathbb{N}$. Then $0 \equiv |\mathrm{supp}(x + y) \cap A| = |\mathrm{supp}(x) \cap A| + |\mathrm{supp}(y) \cap A| \equiv i + 0 \pmod n$ so $i = 0$. That is $D = C$.

By a nearly identical proof one can also establish that for any $m \in \mathbb{Z}$ and any $n \in \mathbb{N}$

$$\begin{aligned}&\{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv m \pmod n\} \in \varphi(m) \text{ and}\\ &\{x \in \mathbb{N} : |\mathrm{supp}(x) \cap B| \equiv m \pmod n\} \in \psi(m)\,.\end{aligned}$$

Notice in particular that this shows that if $k \neq m$ in $\mathbb{Z}$, then $\psi(k) \neq \psi(m)$ and $\varphi(k) \neq \varphi(m)$.

Now suppose that $c\ell\big\{\varphi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \cap c\ell\big\{\psi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \neq \emptyset$. Then by [1, Theorem 3.40] either $\big\{\varphi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \cap c\ell\big\{\psi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \neq \emptyset$ or $\big\{\psi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \cap c\ell\big\{\varphi(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \neq \emptyset$. Assume without loss of generality that the former holds and pick $m \in \mathbb{Z} \setminus \{0\}$ such that $\varphi(m) \in c\ell\big\{\psi(n) : n \in \mathbb{Z} \setminus \{0\}\big\}$. But $c\ell\{x \in \mathbb{N} : |\mathrm{supp}(x) \cap A| \equiv m \pmod{|m| + 1}\}$ is a neighborhood of $\varphi(m)$ which misses $\{\psi(n) : n \in \mathbb{Z}\}$, a contradiction.

To complete the proof, we may assume that $q \notin c\ell\big\{\varphi(n) : n \in \mathbb{Z} \setminus \{0\}\big\}$. Pick a neighborhood U of q which misses $\big\{\varphi(n) : n \in \mathbb{Z} \setminus \{0\}\big\}$. Given $n \in \mathbb{Z} \setminus \{0\}$, U is a neighborhood of $\varphi(n) + \varphi(-n)$ so pick a neighborhood V of $\varphi(n)$ such that $V + \varphi(-n) \subseteq U$. Then $V \cap \big\{\varphi(m) : m \in \mathbb{Z} \setminus \{n\}\big\} = \emptyset$. $\square$

We now introduce a technique which we will use again in the next section.

2.2 Corollary. *Let $q = q + q \in K(\beta\mathbb{N})$. For each $p \in \mathbb{N}^* \cap \overline{\{2^n : n \in \mathbb{N}\}}$ let φ_p be the homomorphism from $\mathbb{Z}$ to the group $q + \beta\mathbb{N} + q$ for which $\varphi_p(1) = q + p + q$. If $p \neq r \in \mathbb{N}^* \cap \overline{\{2^n : n \in \mathbb{N}\}}$, then $c\ell\big\{\varphi_p(n) : n \in \mathbb{Z} \setminus \{0\}\big\} \cap c\ell\big\{\varphi_r(n) : n \in \mathbb{Z} \setminus \{0\}\big\} = \emptyset$ and for all but at most one $p \in \mathbb{N}^*$, $\{\varphi_p(n) : n \in \mathbb{Z}\}$ is a discrete copy of $\mathbb{Z}$.*

Proof. Let $p \neq r \in \mathbb{N}^* \cap \overline{\{2^n : n \in \mathbb{N}\}}$, pick disjoint subsets A and B of $\mathbb{N}$ such that $\{2^n : n \in A\} \in p$ and $\{2^n : n \in B\} \in r$, and apply Theorem 2.1. $\square$

It seems to us inconceivable that there should be *any* $p \in \mathbb{N}^*$ for which $c\ell\{\varphi_p(n) : n \in \mathbb{Z}\}$ is not discrete. But we cannot prove that this cannot happen.

3. Discrete free groups and semigroups in $\mathbb{N}^*$

We show here that each maximal group in the smallest ideal of $\beta\mathbb{N}$ contains $2^{\mathfrak{c}}$ copies, disjoint except at the identity, of the free group on 2 generators (and hence of the free group on countably many generators).

3.1 Lemma. *There is a compact topological group C which contains a free group F on the distinct generators $\{a_1, a_2, a_3, a_4\}$.*

Proof. This is well known. See for example [1, Theorem 2.24]. $\square$

3.2 Lemma. *Let C and F be as in Lemma* 3.1*. Let A_1, A_2, A_3, and A_4 be pairwise disjoint infinite subsets of $\mathbb{N}$ and let $q \in K(\beta\mathbb{N})$. For $i \in \{1,2,3,4\}$ pick*

$$u_i \in \mathbb{N}^* \cap c\ell\{2^n : n \in A_i\}$$

and let $r_i = q + u_i + q$. Let G be the subgroup of $q + \beta\mathbb{N} + q$ generated by $\{r_1, r_2, r_3, r_4\}$. There is a continuous homomorphism $\sigma : \{0\} \cup \mathbb{H} \to C$ such that $\sigma_{|G}$ is an isomorphism onto F and $\sigma(r_i) = a_i$ for each $i \in \{1,2,3,4\}$.

Proof. Denote the identity of C by e. Define $f : \omega \to C$ as follows. For $n \in \omega$,

$$f(2^n) = \begin{cases} a_i & \text{if } n \in A_i \\ e & \text{if } n \notin \bigcup_{i=1}^4 A_i \,. \end{cases}$$

Given $L \in \mathcal{P}_f(\omega)$, $f(\sum_{n\in L} 2^n) = \prod_{n\in L} f(2^n)$, where the product is taken in increasing order of indices. And $f(0) = e$. Let $\widetilde{f} : \beta\omega \to C$ be the continuous extension of f and let σ be the restriction of $\widetilde{f}$ to $\{0\} \cup \mathbb{H}$. By [1, Theorem 4.21] applied to the collection $\mathcal{A} = \{2^n\omega : n \in \mathbb{N}\}$, σ is a homomorphism.

To see that $\sigma[G] = F$ it suffices to let $i \in \{1,2,3,4\}$ and show that $\sigma(r_i) = a_i$. Since f is constantly equal to a_i on $\{2^n : n \in A_i\}$ we have that $\sigma(u_i) = a_i$. Since $q + q = q$, $\sigma(q) = e$. Therefore $\sigma(r_i) = ea_ie = a_i$.

Now let $h : F \to G$ be the homomorphism such that $h(a_i) = r_i$ for each $i \in \{1,2,3,4\}$ and note that $h[F] = G$. Then $\sigma \circ h : F \to F$ and $\sigma \circ h(a_i) = a_i$ for each $i \in \{1,2,3,4\}$, so $\sigma \circ h$ is the identity on F so σ is injective. $\square$

3.3 Theorem. *Let A_1, A_2, A_3, A_4, C, F, G, u_1, u_2, u_3, u_4, r_1, r_2, r_3, r_4, and σ be as in Lemma 3.2. Let G_1 be the subgroup of G generated by $\{r_1, r_2\}$ and let G_2 be the subgroup of G generated by $\{r_3, r_4\}$. Then $c\ell(G_1 \setminus \{q\}) \cap c\ell(G_2 \setminus \{q\}) = \emptyset$. If $i \in \{1,2\}$ and $q \notin c\ell(G_i \setminus \{q\})$, then G_i is a discrete copy of F.*

Proof. Suppose that $c\ell(G_1 \setminus \{q\}) \cap c\ell(G_2 \setminus \{q\}) \neq \emptyset$. By [1, Theorem 3.40], either $(G_1 \setminus \{q\}) \cap c\ell(G_2 \setminus \{q\}) \neq \emptyset$ or $(G_2 \setminus \{q\}) \cap c\ell(G_1 \setminus \{q\}) \neq \emptyset$. Assume without loss of generality that $(G_1 \setminus \{q\}) \cap c\ell(G_2 \setminus \{q\}) \neq \emptyset$ and pick w in this intersection. We shall show that $w = q$. Let s_1 and s_2 denote the inverses of r_1 and r_2 in G_1. Pick $m \in \mathbb{N}$ and $p_1, p_2, \ldots, p_m \in \{r_1, r_2, s_1, s_2\}$ such that $w = p_1 + p_2 + \ldots + p_m$.

Define $\theta : \mathbb{N} \to \omega$ by $\theta(n) = \sum\{2^t : t \in \mathrm{supp}(n) \cap (A_1 \cup A_2)\}$ and let $\widetilde{\theta} : \beta\mathbb{N} \to \beta\omega$ be its continuous extension. By [1, Theorem 4.21] $\widetilde{\theta}_{|\mathbb{H}}$ is a homomorphism. Also $\widetilde{\theta}[\mathbb{H}] \subseteq \mathbb{H} \cup \{0\} = \mathrm{domain}(\sigma)$.

For $i \in \{1,2\}$, θ is the identity on $\{2^n : n \in A_i\}$ so $\widetilde{\theta}(u_i) = u_i$ and since $q + q = q$, $\sigma\big(\widetilde{\theta}(q)\big) = e$. Thus for $i \in \{1,2\}$,

$$\begin{aligned} \sigma\big(\widetilde{\theta}(r_i)\big) &= \sigma\big(\widetilde{\theta}(q + u_i + q)\big) \\ &= e\sigma(u_i)e \\ &= \sigma(q + u_i + q) \\ &= \sigma(r_i)\,. \end{aligned}$$

Also $\sigma\big(\widetilde{\theta}(s_i)\big) = \sigma\big(\widetilde{\theta}(r_i)\big)^{-1} = \sigma(s_i)$.

Next we note that for $i \in \{3,4\}$, $\sigma\big(\widetilde{\theta}(r_i)\big) = e$ for which it suffices to observe that $\widetilde{\theta}(u_i) = 0$ so $\widetilde{\theta}(r_i) = \widetilde{\theta}(q) + 0 + \widetilde{\theta}(q) = \widetilde{\theta}(q)$.

We thus have that $\sigma \circ \widetilde{\theta}[G_2] = \{e\}$ and thus $\sigma\big(\widetilde{\theta}(p_1 + p_2 + \ldots + p_m)\big) = e$. But $\sigma\big(\widetilde{\theta}(p_1 + p_2 + \ldots + p_m)\big) = \sigma(p_1 + p_2 + \ldots + p_m)$ and σ is an isomorphism on G so $p_1 + p_2 + \ldots + p_m = q$.

As in the proof of Theorem 2.1 we have that if $i \in \{1,2\}$ and $q \notin c\ell(G_i \setminus \{q\})$, then G_i is a discrete copy of F. □

3.4 Corollary. *Let $q = q + q \in K(\beta\mathbb{N})$. There exist $2^{\mathfrak{c}}$ copies of the free group on 2 generators in $(q + \beta\mathbb{N} + q) \cap \mathbb{H}$. The intersection of the closures of any two of these is $\{q\}$.*

Proof. Partition $\mathbb{N}^* \cap \overline{\{2^n : n \in \mathbb{N}\}}$ into two element subsets $H_\alpha = \{x_\alpha, y_\alpha\}$ for $\alpha < 2^{\mathfrak{c}}$. For each $\alpha < 2^{\mathfrak{c}}$, let G_α be the subgroup of $q + \beta\mathbb{N} + q$ generated by $q + x_\alpha + q$ and $q + y_\alpha + q$. If $\alpha < \beta < 2^{\mathfrak{c}}$, we can choose disjoint subsets A_1, A_2, A_3, A_4 of $\mathbb{N}$ such that

$\{2^n : n \in A_1\}, \{2^n : n \in A_2\}, \{2^n : n \in A_3\}, \{2^n : n \in A_4\}$ are members of $x_\alpha, y_\alpha, x_\beta, y_\beta$ respectively. So, by Theorem 3.3, there is at most one $\alpha < 2^{\mathfrak{c}}$ for which there is some $\delta \neq \alpha$ with $c\ell(G_\alpha \setminus \{q\}) \cap c\ell(G_\delta \setminus \{q\}) \neq \emptyset$. □

Since the free group on 2 generators contains a copy of the free group on countably many generators, Corollary 3.4 remains valid if "2" is replaced by "countably many". (If G is the free group on the generators $\{a, b\}$, then $\{a^n b^n : n \in \mathbb{N}\}$ generates a free group on countably many generators.)

Recall that a semigroup $(S, \cdot)$ is *weakly left cancellative* provided for all $a, b \in S$, $\{x \in S : ax = b\}$ is finite.

3.5 Corollary. *Let S be an infinite discrete right cancellative and weakly left cancellative semigroup. Let U be a G_δ subset of $\beta S \setminus S$ which contains an idempotent. There is a set $D \subseteq U$ of idempotents such that $|D| = 2^{\mathfrak{c}}$ and for each $q \in D$ there exist $2^{\mathfrak{c}}$ copies of the free group on 2 generators in $q \cdot \beta S \cdot q$. The intersection of the closures of any two of these is $\{q\}$.*

Proof. By [1, Theorem 6.32] U contains a copy of $\mathbb{H}$ so Corollary 3.4 applies. □

Note that one can take $U = \beta S \setminus S$ in Corollary 3.5, so any right cancellative and weakly left cancellative semigroup S has these discrete copies of the free group on 2 generators in $\beta S \setminus S$.

Notice that one cannot have a discrete subset D of $\beta\mathbb{N}$ with $|D| > \mathfrak{c}$ since there are only $\mathfrak{c}$ sets of the form $c\ell A$ for $A \subseteq \mathbb{N}$, and these form a basis for the topology of $\beta\mathbb{N}$. We do not know whether there is any discrete copy of a free group on uncountably many generators in $\beta\mathbb{N}$. We do have the following. Recall that a subset D of a topological space X is *strongly discrete* provided there is an indexed family $\langle U_x \rangle_{x \in D}$ such that for each $x \in D$, U_x is a neighborhood of x and $U_x \cap U_y = \emptyset$ when $x \neq y$.

3.6 Theorem. *There is a strongly discrete copy of the free semigroup with identity on $\mathfrak{c}$ generators in $\mathbb{H}$ (which is therefore discrete in $\mathbb{N}^*$).*

Proof. Pick an indexed family $\langle A_\alpha \rangle_{\alpha < \mathfrak{c}}$ of almost disjoint subsets of $2\mathbb{N} + 1$. (That is, each A_α is infinite and if $\alpha \neq \delta$, then $A_\alpha \cap A_\delta$ is finite.) For each $\alpha < \mathfrak{c}$ pick $p_\alpha \in \mathbb{N}^* \cap c\ell\{2^n : n \in A_\alpha\}$. Pick $q = q + q \in c\ell\{x \in \mathbb{N} : \mathrm{supp}(x) \subseteq 2\mathbb{N}\}$. (We have that $\mathbb{H} \cap c\ell\{x \in \mathbb{N} : \mathrm{supp}(x) \subseteq 2\mathbb{N}\}$ is a compact subsemigroup of $\beta\mathbb{N}$, so has an idempotent.) For $\alpha < \mathfrak{c}$ let $r_\alpha = q + p_\alpha + q$ and let $S = \{q\} \cup \{r_\alpha : \alpha < \mathfrak{c}\}$. Note that $S \subseteq \mathbb{H}$.

For each finite sequence $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$ in $\mathfrak{c}$, let $B_{(\alpha_1, \alpha_2, \ldots, \alpha_k)} = \{x \in \mathbb{N} : \mathrm{supp}(x) \cap (2\mathbb{N} + 1) = \{n_1, n_2, \ldots, n_k\}$ where $n_1 < n_2 < \ldots < n_k$ and each $n_i \in A_{\alpha_i}\}$. Notice that if $k > 1$, then $B_{(\alpha_1,\alpha_2,\ldots,\alpha_{k-1})} \subseteq \{x \in \mathbb{N} : -x + B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)} \in r_{\alpha_k}\}$. (One establishes this statement by an argument similar to that used in the proof of Theorem 2.1 to show that $C \in \psi(m)$ for all m.) Consequently one sees by induction on k that for each $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$, $B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)} \in r_{\alpha_1} + r_{\alpha_2} + \ldots + r_{\alpha_k}$.

Let $C = \{x \in \mathbb{N} : \text{supp}(x) \subseteq 2\mathbb{N}\}$. Note that for each $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle$, $C \cap B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)} = \emptyset$. To complete the proof we show that if $\langle \alpha_1, \alpha_2, \ldots, \alpha_k \rangle \neq \langle \delta_1, \delta_2, \ldots, \delta_l \rangle$, then $\overline{B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)}} \cap \overline{B_{(\delta_1,\delta_2,\ldots,\delta_l)}} \cap \mathbb{H} = \emptyset$. If $k \neq l$, then $B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)} \cap B_{(\delta_1,\delta_2,\ldots,\delta_l)} = \emptyset$, so assume that $k = l$ and pick $i \in \{1, 2, \ldots, k\}$ such that $\alpha_i \neq \delta_i$. Pick $m \in \mathbb{N}$ such that $A_{\alpha_i} \cap A_{\delta_i} \subseteq \{1, 2, \ldots, m\}$. Then $B_{(\alpha_1,\alpha_2,\ldots,\alpha_k)} \cap B_{(\delta_1,\delta_2,\ldots,\delta_l)} \cap 2^{m+1}\mathbb{N} = \emptyset$. □

Strongly discrete subsets of $\mathbb{N}^*$ of size $\mathfrak{c}$ are easy to come by. (The set $\{p_\alpha : \alpha < \mathfrak{c}\}$ in the proof above is one such.) The question naturally arises whether one can get a copy of a free semigroup on $\mathfrak{c}$ (or just uncountably many) generators which is strongly discrete in $\mathbb{N}^*$. The following simple result provides a strong negative answer. In fact there does not exist a strongly discrete uncountable subsemigroup S of $\mathbb{N}^*$ for which there is an element of $\mathbb{N}^*$ right cancellable on S. In particular, an uncountable subsemigroup of $\mathbb{N}^*$ which has an identity cannot be strongly discrete in $\mathbb{N}^*$.

3.7 Theorem. *There do not exist $p \in \mathbb{N}^*$ and a sequence $\langle r_\alpha \rangle_{\alpha<\omega_1}$ in $\mathbb{N}^*$ such that $r_\alpha + p \neq r_\delta + p$ whenever $\alpha < \delta < \omega_1$ and $\{r_\alpha + p : \alpha < \omega_1\}$ is strongly discrete in $\mathbb{N}^*$.*

Proof. Suppose we have such p and $\langle r_\alpha \rangle_{\alpha<\omega_1}$. Choose for each $\alpha < \omega_1$ some $B_\alpha \in r_\alpha + p$ such that $B_\alpha \cap B_\delta$ is finite whenever $\alpha < \delta < \omega_1$. For each $\alpha < \omega_1$ let $C_\alpha = \{x \in \mathbb{N} : -x + B_\alpha \in p\}$ and note that $C_\alpha \in r_\alpha$. The collection $\{C_\alpha : \alpha < \omega_1\}$ cannot be pairwise disjoint so pick $\alpha < \delta < \omega_1$ such that $C_\alpha \cap C_\delta \neq \emptyset$ and pick $x \in C_\alpha \cap C_\delta$. Then $(-x + B_\alpha) \cap (-x + B_\delta) \in p$ and is therefore infinite, and consequently $B_\alpha \cap B_\delta$ is infinite. □

We close with the following questions.

3.8 Question. *Is there a discrete copy of $\mathbb{Z}$ in $\mathbb{N}^*$ which is not contained in $\mathbb{H}$?*

3.9 Question. *Are there discrete copies of a free semigroup on uncountably many generators (with or without identity) contained in the maximal groups of $K(\beta\mathbb{N})$?*

3.10 Question. *Are there groups not contained in the free group on 2 generators for which there are discrete copies in $\beta\mathbb{N}$?*

The discrete groups produced in this paper are the first examples of which we are aware of nontrivial topological groups in $\beta\mathbb{N}$.

3.11 Question. *Are there any nondiscrete topological groups contained in $\beta\mathbb{N}$?*

We observe that any countable topological group contained in $\beta\mathbb{N}$ has to be discrete. To see this note that any countable subset of $\beta\mathbb{N}$ is extremally disconnected. (This is immediate from [1, Theorem 3.40].) V. I. Malyhin has shown that every non-discrete extremally disconnected topological group has an open subgroup of exponent two [3]. By Zelenyuk's Theorem ([4] or see [1, Theorem 7.17]), a group of this kind cannot be embedded algebraically in $\mathbb{N}^*$, because it contains subgroups of order 2.

We remark that there is a simple direct proof that, if $q = q+q \in \mathbb{N}^*$, the group $\mathbb{Z}+q$ contained in $\mathbb{N}^*$, cannot be a topological group. We have already remarked that it is not discrete. To see that it is not a topological group, let $A = \{n \in \mathbb{N} : \min\big(\mathrm{supp}(n)\big) \in 2\omega+1\}$ and let $B = \{n \in \mathbb{N} : \min\big(\mathrm{supp}(n)\big) \in 2\omega\}$. Using the fact that $q \in \mathbb{H}$ [1, Lemma 6.8], it is easy to check that, for any $n \in \mathbb{Z}$, $n + q \in \overline{A}$ implies that $2n + q \in \overline{B}$ and vice-versa. Pick a net $\langle n_\iota \rangle_{\iota \in D}$ in $\mathbb{Z} \setminus \{0\}$ such that $\langle n_\iota + q \rangle_{\iota \in D}$ converges to q. If $\mathbb{Z} + q$ were a topological group, we would have that $\langle 2n_\iota + q \rangle_{\iota \in D}$ also converges to q because $q = q + q$ and for $\iota \in D$, $n_\iota + q + n_\iota + q = 2n_\iota + q$.

References

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

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

[3] V. Malyhin, *Extremally disconnected and nearly extremally disconnected topological groups (Russian)*, Dokl. Nauk. SSSR **220** (1975), 27-30. (English translation: Soviet Math. Dokl. **16** (1975), 21-25.)

[4] Y. Zelenyuk, *Topological groups with finite semigroups of ultrafilters* (Russian), Matematychni Studii **6** (1996), 41-52.

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`