HINDMAN'S THEOREM AND IDEMPOTENT TYPES

URI ANDREWS AND ISAAC GOLDBRING

Abstract. Motivated by a question of Di Nasso, we show that Hindman's Theorem is equivalent to the existence of idempotent types in countable complete extensions of Peano Arithmetic.

Keywords: Hindman's theorem, idempotent types

1. Introduction

Recall that $X \subseteq \mathbb{N}$ is said to be an *IP set* if there is infinite $Y \subseteq X$ such that every finite sum of distinct elements of Y is in X. Hindman's Theorem asserts that if $\mathbb{N}$ is partitioned into finitely many pieces, then one of the pieces is an IP set.

Hindman's original proof was very combinatorial in nature. Later, Galvin and Glazer gave a "soft" proof of Hindman's theorem using the notion of an *idempotent ultrafilter*. Recall that an ultrafilter $\mathcal{U}$ on $\mathbb{N}$ is said to idempotent if, for all $A \subseteq \mathbb{N}$, we have

$$A \in \mathcal{U} \Leftrightarrow \{n \in \mathbb{N} \ : \ A - n \in \mathcal{U}\} \in \mathcal{U};$$

here, $A - n := \{x \in \mathbb{N} \ : \ x + n \in A\}$. It just takes an easy induction to verify that all sets in an idempotent ultrafilter are IP sets, so to establish Hindman's theorem, it suffices to establish the existence of an idempotent ultrafilter. This latter task can be accomplished via several applications of Zorn's Lemma and essentially boils down to Ellis' theorem about compact semi-topological semigroups.

In [1], Di Nasso asks whether or not there can be a "nonstandard" proof of the existence of idempotent ultrafilters, presumably using only the same amount of choice needed to prove the existence of ordinary nonprincipal ultrafilters. Towards this end, Di Nasso and Tachtsis [2] recently showed that the existence of idempotent ultrafilters follows from ZF along with the Ultrafilter Theorem on $\mathbb{R}$. In order to formulate an attack on this problem, he establishes a purely model-theoretic formulation of the existence of idempotent ultrafilters: In a model of nonstandard analysis, there exists $\alpha, \beta \in \mathbb{N}^*$ satisfying the following two properties:

- for all $A \subseteq \mathbb{N}$, we have $\alpha \in A^* \Leftrightarrow \beta \in A^* \Leftrightarrow \alpha + \beta \in A^*$;
- for all $B \subseteq \mathbb{N}^2$, if $(\alpha, \beta) \in B^*$, then there is $n \in \mathbb{N}$ such that $(n, \beta) \in B^*$.

When there is a pair (α, β) as above, he calls α an *idempotent element* of $\mathbb{N}^*$. Since this terminology is a bit confusing in the sense that such elements are not actually idempotent in the algebraic sense as elements of the semigroup $\mathbb{N}^*$, they have since been renamed to *u-idempotent* elements. DiNasso in fact defines u-idempotent elements in models of complete extension of Peano Arithmetic (PA) and asks for a sufficient condition to guarantee the existence of u-idempotent elements in such models (with an eye towards an answer to his earlier question).

The main result of this note is that Hindman's theorem is actually equivalent to the existence of idempotent *types* in arbitrary *countable* complete extensions of PA, where an idempotent type is simply the type of a u-idempotent element (we give a realization-free definition below); in particular, idempotent types always exist in such theories. (We actually use the version of Hindman's theorem that states that the family of IP sets is *partition regular*, meaning that if $X \subseteq \mathbb{N}$ is an IP set and Y is a subset of X, then either Y or $X \setminus Y$ is an IP set. Accordingly, we show that idempotent types containing a prescribed 0-definable IP set always exist.)

It is not clear to us if the existence of idempotent types in all countable complete extensions of PA can be used to obtain idempotent ultrafilters using some sort of compactness argument. Conversely, it follows from Lemma 2.6 below that from idempotent ultrafilters we can obtain idempotent types.

The main results in this note seem to have departed from DiNasso's original question in two ways: we work with types rather than elements and in countable languages rather than the uncountable language of nonstandard analysis. Since u-idempotent elements are realizations in elementary extensions of idempotent types, the former deviation seems to be of little concern in constructive matters. For the latter deviation, in many cases, one often does not use the full strength of idempotency of an ultrafilter but rather its idempotency with respect to countably many sets that are of use for the problem at hand, and thus this change in perspective is often benign.

Hindman's theorem and idempotent ultrafilters actually make sense in the much more general context of semigroups and so we prove all of our results in this more general context.

Since foundational issues are of central importance in this paper, it is important to note that all of our results proven are theorems of ZF. For an even finer analysis of the reverse mathematics of the situation, see Remark 3.5.

We would like to thank the anonymous referee for numerous helpful comments and suggestions, including a more streamlined proof of our main result.

2. Definitions

By a *semigroup structure* we mean a first-order structure $\mathcal{M} := (M, \cdot, \ldots)$ in a countable language such that $(M, \cdot)$ is a semigroup; in this case, we say that $\mathcal{M}$ is *based on* $(M, \cdot)$.

Definition 2.1. We say $q(x, y) \in S_2(M)$ is an *independent type* if, for any $\varphi(x, y) \in q$, there is $u \in M$ such that $\varphi(u, y) \in q$.

Here, $S_2(M)$ denotes the set of complete 2-types over M.

Remark 2.2. *In model-theoretic terminology, independent types are simply heirs. More precisely, if (a, b) realizes q (in some elementary extension of $\mathcal{M}$), then q is independent if and only if* $\mathrm{tp}(b/Ma)$ *is an heir of* $\mathrm{tp}(b/M)$.

Definition 2.3. $p(x) \in S_1(M)$ is called an *idempotent type* if there is an independent type $q(x, y)$ such that $p(x), p(y), p(x \cdot y) \subseteq q(x, y)$.

Remark 2.4. *In the definition of idempotent type, we do not insist that the type be non-principal. In fact, an idempotent type $p(x) \in S_1(M)$ is principal if and only if $p(x) = \mathrm{tp}(a/M)$ for $a \in M$ idempotent. We will have more to say about this at the end of the paper.*

Remark 2.5. *Recall that the (model-theoretic)* completion *of $\mathbb{N}$ is the structure $\mathbb{N}^{\#}$ with a symbol for every function and relation on $\mathbb{N}$ and a symbol for every element of $\mathbb{N}$. In* [1]*, it is shown that*

if $T^{\#} := \mathrm{Th}(\mathbb{N}^{\#})$, then by identifying a type with the set of definable sets defined by formulas in the type, idempotent types for $T^{\#}$ are precisely the idempotent ultrafilters on $\mathbb{N}$. The same observation (with an identical proof) actually holds for arbitrary semigroup structures.

The following reformulation of idempotent type will prove useful in the next section. It is in fact the type generalization of the fact proved in [1] that an ultrafilter $\mathcal{U}$ on $\mathbb{N}$ is idempotent if and only if: for every $A \in \mathcal{U}$, there is $a \in A$ such that $A - a \in \mathcal{U}$.

Lemma 2.6. *A type $p(x) \in S_1(M)$ is idempotent if and only if: for every $\varphi(x) \in p(x)$, there is $u \in M$ so that $\varphi(u) \wedge \varphi(u \cdot x) \in p(x)$.*

Proof. First we suppose that $p(x)$ is an idempotent type. Let $q(x, y)$ be an independent type which witnesses this and fix $\varphi(x) \in p(x)$. Then $\varphi(x) \wedge \varphi(x \cdot y) \in q(x, y)$ since $p(x) \cup p(y) \cup p(x \cdot y) \subseteq q(x, y)$. Then, since $q(x)$ is independent, we have that there is some $u \in M$ so that $\varphi(u) \wedge \varphi(u \cdot y) \in q(x, y)$. Finally, since $p(y) \subseteq q(x, y)$, we have that $\varphi(u) \wedge \varphi(u \cdot y) \in p(y)$. Changing variables from y to x yields the result.

Now, suppose that for every $\varphi(x) \in p(x)$, there is $u \in M$ so that $\varphi(u) \wedge \varphi(u \cdot x) \in p(x)$. We say that $\varphi(x, y)$ is represented if for some $u \in M$, $\varphi(u, x) \in p(x)$. We first check that

$$p(x) \cup p(y) \cup p(x \cdot y) \cup \{\neg\psi(x, y) \mid \psi(x, y) \text{ is not represented}\}$$

is consistent. Towards this end, we need only check that $\varphi(x) \wedge \varphi(y) \wedge \varphi(x \cdot y) \wedge \bigwedge_{i \leq n} \neg\psi_i(x, y)$ is consistent, where $\varphi(x) \in p(x)$ and each $\psi_i(x, y)$ is not represented. By hypothesis, we know that there is $u \in M$ so that $\varphi(u) \wedge \varphi(u \cdot x) \in p(x)$, whence we also have $\varphi(u) \wedge \varphi(x) \wedge \varphi(u \cdot x) \in p(x)$. Since each $\psi_i(x, y)$ is not represented, we have that $\neg\psi_i(u, x) \in p(x)$ for each i. It follows that $\varphi(u) \wedge \varphi(x) \wedge \varphi(u \cdot x) \wedge \bigwedge_{i \leq n} \neg\psi_i(u, x) \in p(x)$, showing our needed consistency.

Now, let $q(x, y)$ be any type containing $p(x) \cup p(y) \cup p(x \cdot y) \cup \{\neg\psi(x, y) \mid \psi(x, y) \text{ is not represented}\}$. Since $q(x, y)$ only contains formulas $\psi(x, y)$ which are represented, $q(x, y)$ is independent. Since $p(x) \cup p(y) \cup p(x \cdot y) \subseteq q(x, y)$, this shows that $p(x)$ is idempotent. □

We finally recall the main combinatorial notion of the paper.

Definition 2.7. Let $(M, \cdot)$ be a semigroup. If (u_n) is a countable sequence from M, we define $\mathrm{FP}(u_n) := \{u_{i_1} \cdots u_{i_k} \ : \ i_1 < \cdots < i_k\}$. We call $X \subseteq M$ an *IP set* if there is a sequence (u_n) for which $\mathrm{FP}(u_n) \subseteq X$, in which case we refer to (u_n) as a *basis* for X.

3. Main results

In this section, $(M, \cdot)$ denotes an arbitrary countable semigroup.

Statement 3.1 (Hindman's theorem for $(M, \cdot)$)**.** *Let $X \subseteq M$ be an IP-set. Then for any $Y \subseteq X$, either Y or $X \setminus Y$ is an IP-set.*

Statement 3.2 (Existence of idempotent types for semigroup structures based on $(M, \cdot)$)**.** *If $\mathcal{M} = (M, \cdot, \ldots)$ is a semigroup structure based on $(M, \cdot)$ and $X \subseteq M$ is an $\mathcal{M}$-definable IP-set, then there is an idempotent type over $\mathcal{M}$ containing X.*

Theorem 3.1. *Statement 3.1 is equivalent to Statement 3.2.*

Before proving Theorem 3.1, we will state and prove the following consequence of Statement 3.1:

Lemma 3.3. *Let M be a semigroup satisfying Statement 3.1 and $X \subseteq M$ be an IP-set. Let $(A_n \mid n \geq 1)$ be any countable collection of subsets of M. Then there exists:*

- *a sequence of IP-sets $(Z_n \mid n \geq 1)$;*
- *a non-increasing sequence of IP-sets $X = B_0 \supseteq B_1 \supseteq B_2 \supseteq \cdots$;*
- *a sequence of elements $(y_n \mid n \geq 1)$ of M;*

so that for each $n \geq 1$, the following hold:

(1) $Z_n = A_n$ or $M \setminus A_n$;
(2) $y_n \in Z_n \cap B_{n-1}$;
(3) $B_n \subseteq Z_n \cap (Z_n/y_n)$, i.e. for every $x \in B_n$, we have $x, y_n \cdot x \in Z_n$.

Proof. Set $B_0 = X$. Suppose that we have defined Z_n, B_n, and y_n for all $1 \leq n < k$ so that the three conditions are satisfied for each $1 \leq n < k$.

Set $Z_k = A_k$ if and only if $A_k \cap B_{k-1}$ is an IP-set, and otherwise set $Z_k = M \setminus A_k$. By Statement 3.1, $Z_k \cap B_{k-1}$ is an IP-set. Let $\mathrm{FP}(x_n)_{n\geq 1}$ be contained in $Z_k \cap B_{k-1}$ for some infinite sequence $(x_n \mid n \geq 1)$. Set $B_k = \mathrm{FP}(x_n)_{n\geq 2}$ and let $y_k = x_1$. It is clear that these choices of B_k, Z_k, and y_k satisfy the conditions (1)-(3).

□

Proof that Statement 3.1 implies Statement 3.2: Let $(A_n \mid n \geq 1)$ enumerate all $L(M)$-definable subsets of M such that each definable set is enumerated infinitely often. The previous lemma yields a sequence of definable sets $(Z_n \mid n \geq 1)$ so that $Z_n = A_n$ or $Z_n = M \setminus A_n$. Let $\mathcal{F} = \{Z_n \mid n \geq 1\}$ and define a 1-type $p(x)$ by $\varphi(x) \in p(x)$ if and only if the set defined by $\varphi(x)$ is in $\mathcal{F}$. Note that $p(x)$ is consistent as the intersection of $(Z_i \mid i \leq n)$ must contain B_n, which is an IP-set, and is thus non-empty.

We now claim that $p(x)$ satisfies the condition of Lemma 2.6. Suppose that $\varphi(x) \in p(x)$ defines Z_n. We claim that $\varphi(y_n \cdot x) \in p(x)$ as well. Take $m > n$ such that A_m is the set defined by $\varphi(y_n \cdot x)$. It remains to note that at stage m, we could not have set Z_m to be equal to $M \setminus A_m$. Indeed, every $z \in B_n$ has the property that $y_n \cdot z \in Z_n$, whence $B_n \subseteq A_m$ and thus $B_m \cap (M \setminus A_m) \subseteq B_n \cap (M \setminus A_m) = \emptyset$, which is not an IP-set. □

Proof that Statement 3.2 implies Statement 3.1: Fix an IP set $X \subseteq M$ and fix $Y \subseteq X$. Let $\mathcal{L}$ denote the language by $\{\cdot, X, Y\}$ and consider the semigroup structure $\mathcal{M} := (M, \cdot, X, Y)$. Let $p(x)$ be an idempotent type contained in the independent type $q(x, y)$ containing the formula $X(x)$. Without loss of generality, we may assume $Y(x)$ belongs to p (otherwise re-name Y to define $X \setminus Y$).

Set $\psi_1(x, y) := Y(x) \wedge Y(x \cdot y)$. Since q witnesses that p is idempotent, we have that $\psi_1(x, y) \in q$. Since q is independent, there is a $u_1 \in M$ so that $\psi_1(u_1, y) \in q$. Again, since q witnesses that p is idempotent, $Y(u_1 \cdot x) \wedge Y(u_1 \cdot x \cdot y) \in q$.

Let $\psi_2(x, y) := \psi_1(x, y) \wedge \psi_1(u_1 \cdot x, y)$. Since $\psi_2(x, y)$ belong to q, there is $u_2 \in M$ so that $\psi_2(u_2, y) \in p$. We now have that $u_1, u_2, u_1 \cdot u_2 \in Y$. Moreover, $\psi_2(u_2, x) \wedge \psi_2(u_2, x \cdot y) \in q$ Continuing in this manner, we construct a sequence $(u_i \mid i \in \omega)$ which is a basis for Y. □

Remark 3.4. The proof that Statement 3.2 implies Statement 3.1 is more or less Galvin's half of the Galvin-Glazer proof of Hindman's theorem (written in first-order formalism). On the other

hand, Hindman originally had proven the existence of an idempotent ultrafilter on $\mathbb{N}$ from the Continuum Hypothesis in [4] and it is unclear to us if there is any connection between his argument and our proof that Statement 3.1 implies Statement 3.2.

Remark 3.5. Concerning the reverse mathematical strength of our result, our result shows the equivalence over RCA_0 of the existence of idempotent types (Statement 3.2 above) and the so-called *Iterated Hindman's Theorem*, which says that if (X_i) is an infinite sequence of subsets of M, then there exists a sequence (y_i) so that for each k, $\mathrm{FP}((y_i)_{i\geq k}) \subseteq X_k$ or $\mathrm{FP}((y_i)_{i\geq k}) \subseteq M \setminus X_k$. We do not pursue this notation or formalism, preferring rather to simply informally allow repeated uses of Hindman's theorem (Statement 3.1) in our proofs. The proofs given above can be routinely formalized in this language.

4. Musings on non-principality

As mentioned above, in certain semigroups, IP sets can be finite, even singletons. Likewise, idempotent types can be principal. We mention here some conditions on semigroups that remove some of these trivialities.

Here are two possible ways of making the notion of IP less trivial.

Definition 4.1. Suppose that $(M,\cdot)$ is a semigroup and $A \subseteq M$.

(1) We say that A is IIP (*infinite IP*) if there is a sequence (x_n) such that $\mathrm{FP}(x_n) \subseteq A$ and $\mathrm{FP}(x_n)$ is infinite.
(2) We say that A is DIP (*distinctly IP*) if there is an injective sequence (x_n) with $\mathrm{FP}(x_n) \subseteq A$.

Clearly DIP sets are IIP. A class of semigroups where DIP is a good notion can be found in the literature:

Definition 4.2. (Golan and Tsaban, [3]) We call a semigroup $(M,\cdot)$ *moving* if $\beta M \setminus M$ is a subsemigroup of βM.

There is a more combinatorial definition of moving semigroup, but let us be content with the ultrafilter definition.

Lemma 4.3. *If $(M,\cdot)$ is moving, then $A \subseteq M$ is DIP if and only if there is a* nonprincipal *idempotent ultrafilter $\mathcal{U}$ on S containing A.*

Proof. If A is DIP as witnessed by (x_n), then $T := \bigcap_{n=m}^{\infty}(\overline{\mathrm{FP}(x_n)_{n=m}^{\infty}} \cap (\beta S \setminus S))$ is a nonempty compact subsemigroup of βS. If $\mathcal{U} \in T$ is idempotent, then $A \in \mathcal{U}$. The converse follows from the usual argument, using the fact that one can always find a fresh element at every stage of the construction. □

Corollary 4.4. *In moving semigroups, the notion of being DIP is partition regular.*

Observe that in a moving semigroup, to conclude that A belonged to a nonprincipal idempotent ultrafilter, all that was really used was that A was IIP. It thus follows that:

Corollary 4.5. *In moving semigroups, the notions IIP and DIP coincide.*

Here is an admittedly ad hoc definition:

Definition 4.6. We call a semigroup $(M, \cdot)$ *Hindman* if the notion of being IIP is partition regular.

It follows from the above corollaries that moving semigroups are Hindman.

The following theorem follows immediately from the proofs in the preceding section:

Theorem 4.7. *Let $(M, \cdot)$ be a semigroup.*

(1) Suppose that $(M, \cdot)$ is Hindman and $\mathcal{M}$ is a semigroup structure based on $(M, \cdot)$. Then for every $\mathcal{M}$-definable $X \subseteq M$ that is IIP, there is a nonprincipal *idempotent type containing the formula $X(x)$.*

(2) Suppose that for every semigroup structure $\mathcal{M}$ based on $(M, \cdot)$ and every $\mathcal{M}$-definable $X \subseteq M$ that is IIP, there is a nonprincipal idempotent type containing $X(x)$. Then $(M, \cdot)$ is really *Hindman, meaning that whenever $X \subseteq M$ is IIP and $X = Y \cup Z$, then one of Y or Z is DIP.*

Corollary 4.8. *In Hindman semigroups, the notions IIP and DIP coincide.*

Question 4.9. *Do the notions IIP and DIP coincide in every semigroup? Does the property that the DIP sets are partition regular characterize moving semigroups? Is every Hindman semigroup moving?*

A positive answer to the second question yields a positive answer to the third question.

References

[1] M. Di Nasso, *Hypernatural numbers as ultrafilters*, Chapter in "Nonstandard Analysis for the Working mathematician" (P.A. Loeb and M. Wolff, eds.), 2nd edition, Springer, 2015

[2] M. Di Nasso and E. Tachtsis, *Idempotent ultrafilters without Zorn's Lemma*, Proc. A.M.S. **146** (2018), 397-411

[3] G. Golan and B. Tsaban, *Hindman's coloring theorem in arbitrary semigroups*, Journal of Algebra 395 (2013), 111-120.

[4] N. Hindman, *The existence of certain ultra-filters on $\mathbb{N}$ and a conjecture of Graham and Rothschild*, Proc. A.M.S. **36** (1972), 341-346.

Department of Mathematics, University of Wisconsin, Madison, WI 53706-1388, USA

E-mail address: andrews@math.wisc.edu

URL: http://www.math.wisc.edu/~andrews/

Department of Mathematics, University of California, Irvine, 340 Rowland Hall (Bldg.# 400), Irvine, CA 92697-3875

E-mail address: isaac@math.uci.edu

URL: homepages.math.uci.edu/~isaac/