

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.

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 be 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 is readily verified 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 [2], 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. In order to formulate an attack on this problem, he establishes a purely model-theoretic formulation of the existence of idempotent ultrafilters: 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 $(n, \beta) \in B^*$.

By replacing A and B by 0-definable sets relative to some complete theory T extending Peano Arithmetic (PA), it now makes sense to talk about *idempotent types* in such theories. In [2], Di Nasso also asks for a sufficient condition to guarantee the existence of idempotent types in arbitrary complete extensions of PA (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; 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 countable complete extensions of PA can be used to obtain idempotent ultrafilters using some sort of compactness argument. Conversely, it is not clear to us how to use idempotent ultrafilters to obtain idempotent types.

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.

1.1. Constructive consequences. In [4], Tao alludes to the fact that arguments in combinatorics involving idempotent ultrafilters are highly nonconstructive as one needs to use the axiom of choice multiple times to prove the existence of an idempotent ultrafilter. (As a curiosity, it is not currently known whether or not the existence of idempotent ultrafilters on \mathbb{N} is equivalent, over ZF, to the existence of nonprincipal ultrafilters on \mathbb{N} .) In relation to this fact, here is a vague conjecture:

Thesis 1.1. *Any argument in combinatorics utilizing the existence of idempotent ultrafilters could instead use idempotent types.*

If this thesis is true, then by our main result, any argument in combinatorics utilizing idempotent ultrafilters could instead use Hindman's theorem directly; since Hindman's theorem can be proven constructively and our proof that Hindman's theorem implies the existence of idempotent types is also constructive, this would allow all arguments using idempotent ultrafilters to be made constructive. It is not clear how one could prove (or even precisely formulate) the above thesis, but, intuitively speaking, in proving a result about a set A of natural numbers, the argument involved should only mention sets definable from A in second order arithmetic and so an idempotent type in an appropriate countable language should suffice to carry out the argument.

Concerning the reverse mathematical strength of our result, we show that the existence of idempotent types is enough to carry out the usual ultrafilter proof of Hindman's theorem using only RCA_0 . Conversely, proving the existence of idempotent types from Hindman's theorem seems to need to use Π_1^1 -comprehension.

2. DEFINITIONS

By a *semigroup structure* we mean a first-order structure $\mathcal{M} := (M, \cdot, \dots)$ 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 $\varphi(u, y) \in q$.

Remark 2.2. *In model-theoretic lingo, 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 $\text{tp}(b/Ma)$ is an heir of $\text{tp}(b/M)$.*

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 $p(x) \in S(M)$ is principal if and only if $p(x) = \text{tp}(a/M)$ 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 [2], it is shown that*

if $T^\# := \text{Th}(\mathbb{N}^\#)$, then 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.

Definition 2.6. Let (M, \cdot) be a semigroup. If (u_n) is a countable sequence from M , we define $\text{FP}(u_n) := \{u_{i_1} \cdots u_{i_k} : i_1 < \cdots < i_k\}$. We call $X \subseteq M$ an *IP set* if there is a sequence (u_n) for which $\text{FP}(u_n) \subseteq X$, 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 $\mathcal{M} = (M, \cdot, \dots)$ is a semigroup structure based on (M, \cdot) and $X \subseteq M$ is a \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.*

Proof that Statement 3.1 implies Statement 3.2: Let $(\varphi_i(x) : i < \omega)$ enumerate all $L(M)$ -formulae in the free variable x and let $(\psi_j(x, y) : j < \omega)$ enumerate all the $L(M)$ -formulae in the free variables x, y . Without loss of generality, assume that φ_0 is the formula that defines X .

We build an approximation to an independent type q in stages. At every stage s , we build two finite sets of formulae: $A_s(x)$ and $B_s(x, y)$. Throughout the construction, we will maintain the following recursive assumptions:

- (1) For each $i \leq s$, exactly one of φ_i or $\neg\varphi_i$ belongs to A_s ;
- (2) $A_s(x)$ defines an IP subset of M ;
- (3) There is $J_s \subseteq \{0, 1, \dots, s-1\}$ such that $B_s = \{\neg\psi_j : j \in J_s\}$.
- (4) For every $u \in M$ and every $j \in J_s$, $A_s(y) \cup \{\psi_j(u, y)\}$ does not define an IP subset of M .
- (5) For each $j \in \{0, 1, \dots, s-1\} \setminus J_s$, there is $u \in M$ so that $\psi_j(u, y) \in A_s(y)$.

At stage 0, we begin with $A_0(x) = \{\varphi_0(x)\}$ and $B_0 = \emptyset$. Clearly (1)-(5) are satisfied at this stage.

Now assume that the construction has been carried out through stage s and we show how to carry it through to stage $s+1$. First, if $A_s(x) \cup \{\varphi_{s+1}(x)\}$ defines an IP subset of M , then we set $A_{s+1}^0 := A_s(x) \cup \{\varphi_{s+1}(x)\}$. Otherwise, we set $A_{s+1}^0 := A_s(x) \cup \{\neg\varphi_{s+1}(x)\}$. By Statement 3.1, in either case, A_{s+1}^0 defines an IP subset of M .

Now we shift our attention to $\psi_s(x, y)$. If there is $u \in M$ so that $A_{s+1}^0(y) \cup \{\psi_s(u, y)\}$ defines an IP subset of M , then we set $A_{s+1}(y)$ to be this set of formulae (for the least such u with respect to some fixed ordering of M). Otherwise, set $A_{s+1}(y) := A_{s+1}^0(y)$ and put $\neg\psi_s(x, y)$ into B_{s+1} . It is clear that (1)-(5) holds for A_{s+1} and B_{s+1} .

Claim: For each s , $A_s(x) \cup A_s(y) \cup A_s(x \cdot y) \cup B_s(x, y)$ is consistent.

Proof of claim: Set u to be the least element of M (again, with respect some fixed ordering of M) that lies in a basis for the set defined by A_s . It suffices to show that the set of formulae

$$A_s(y) \cup A_s(u \cdot y) \cup B_s(u, y)$$

is consistent. Let Z denote the subset of M defined by $A_s(y) \cup A_s(u \cdot y)$. Since u belongs to a basis for the set defined by A_s , it follows that Z is an IP set. By (4), $Z \cap \psi_j(u, M)$ is not an IP set for each $j \in J_s$. By Statement 3.1, we get that $Z \cap \bigcap_{j \in J_s} \neg \psi_j(u, M)$ is an IP set, whence is nonempty, proving the claim.

By the claim, $q_0(x, y) := \bigcup_s (A_s(x) \cup A_s(y) \cup A_s(x \cdot y) \cup B_s(x, y))$ is a partial type over M . By (1), the restriction of q_0 to the variable x is a complete type $p(x)$ over M and $p(x), p(y), p(x \cdot y) \subseteq q_0(x, y)$. Let $q(x, y) \in S_2(M)$ be any completion of q_0 . It remains to prove that q is independent. Towards this end, fix $\theta(x, y) \in q$. Take s such that $\theta = \psi_s$. Since $\neg \psi_s \notin B_{s+1}$, we have that $s \notin J_{s+1}$, so by (5), there is $u \in M$ such that $\psi_s(u, y) \in A_{s+1}(y)$, whence $\theta(u, y) \in q$. □

Proof that Theorem 3.2 implies Theorem 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 . □

4. MUSINGS ON NON-PRINCIPALITY

As mentioned above, in weird 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 $\text{FP}(x_n) \subseteq A$ and $\text{FP}(x_n)$ is infinite.
- (2) We say that A is DIP (*distinctly IP*) if there is an injective sequence (x_n) with $\text{FP}(x_n) \subseteq A$.

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 $T := \bigcap_{n=m}^{\infty} (\overline{\text{FP}(x_n)_{n=m}^{\infty}} \cap (\beta S \setminus S))$ 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. \square

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] Andreas Blass, Jeffrey Hirst, and Stephen Simpson, *Logical analysis of some theorems of combinatorics and topological dynamics*, Logic and combinatorics, Contemp. Math., 65, Amer. Math. Soc., Providence, RI, 1987
- [2] M. Di Nasso, *Hypernatural numbers as ultrafilters*, to appear as a chapter in “Nonstandard Analysis for the Working mathematician” (P.A. Loeb and M. Wolff, eds.), 2nd edition. arXiv 1501.05755
- [3] G. Golan and B. Tsaban, *Hindman’s coloring theorem in arbitrary semigroups*, Journal of Algebra 395 (2013), 111-120.
- [4] T. Tao, <https://terrytao.wordpress.com/2012/11/28/multiple-recurrence-in-quasirandom-groups/>
- [5] H. Towsner, *A simple proof and some difficult examples for Hindman’s theorem*, Notre Dame J. Formal Logic, **53** (2012), 53-65.

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, STATISTICS, AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO,
SCIENCE AND ENGINEERING OFFICES M/C 249, 851 S. MORGAN ST., CHICAGO, IL, 60607

E-mail address: `isaac@math.uic.edu`

URL: `homepages.math.uic.edu/~isaac/`