HINDMAN'S THEOREM VIA ULTRAFILTERS

LEO GOLDMAKHER

Abstract. A self-contained exposition of the ultrafilter proof of Hindman's theorem. This proof was explained to me by Mike Pawliuk.

1. Motivation

Given a finite coloring of the positive integers, it's clear that there must be some infinite monochromatic set. Is there anything more that can be said, without making any further assumptions? This naive question was a driving force in the creation of Additive Combinatorics, a field which has seen spectacular breakthroughs over the past eighty years and continues to flourish today. One of the first results in the area is the following:

Theorem 1.1 (van der Waerden, 1927)**.** *Given any finite coloring of the positive integers, there exist arbitrarily long monochromatic arithmetic progressions.*

Note that this does *not* say that there exists an infinite monochromatic arithmetic progression. In fact, this is false even using only two colors.

van der Waerden's theorem can be quantified in various ways. For example, must every infinite monochromatic set contain arbitrarily long APs? (If the monochromatic set has positive upper density, Szemerédi's theorem says yes. Can one get away with a weaker assumption? This is an active area of research, with notable recent breakthroughs by Green and Tao, among others.) Or in a different vein: given C colors, how many positive integers must be colored to guarantee that there is a monochromatic arithmetic progression of length L? (Progress has been made thanks to many people, perhaps most notably Bourgain, Gowers, and Roth.) We can also generalize these questions by coloring other objects, such as higher dimensional analogues of the positive integers (the Hales-Jewett theorem), or graphs (Ramsey theory).

In all of the above, the point is to capture some rigid structure inside an infinite monochromatic set. There are many natural questions along similar lines. For example, given a finite coloring of the positive integers, must there be an infinite monochromatic set which is closed under addition? A little thought shows that the answer is no. Nonetheless, a beautiful result of Hindman asserts that we have something almost as good. Given a set A, define $\sum_A$ to be the collection of all distinct sums of elements of A:

$$\sum\nolimits_A := \left\{ \sum_{a \in A_f} a : A_f \text{ is a finite subset of } A \right\}.$$

In particular, note that $A \subseteq \sum_A$, and that $\sum_A$ is finite if and only if A is finite.

Theorem 1.2 (Hindman's theorem)**.** *Given any finite coloring of the positive integers, there exists an infinite monochromatic set A such that the larger set $\sum_A$ is monochromatic.*

The theorem has a number of proofs, in particular a very elegant one in the language of *ultrafilters*. Informally, given an infinite set X, a *filter* on X is a collection of large subsets of X; an *ultrafilter* is a maximal filter. One can think of an ultrafilter as defining what it means for a subset of X to be large, the same way a topology defines what it means for a subset to be open.

To describe the proof of Hindman's theorem, it suffices to know just a few properties of ultrafilters, so we postpone a proper discussion of ultrafilters to Section 2 and focus on the results we require for our application. Let $U(\mathbb{N})$ denote the collection of all ultrafilters on $\mathbb{N}$.

(1) $\mathbb{N} \in \mathcal{F}$ for any ultrafilter $\mathcal{F} \in U(\mathbb{N})$.
(2) For all $\mathcal{F} \in U(\mathbb{N})$, if $A \sqcup B \in \mathcal{F}$ then either $A \in \mathcal{F}$ or $B \in \mathcal{F}$.
(3) $U(\mathbb{N})$ forms a semigroup with respect to a certain operation $\oplus$.

An ultrafilter $\mathcal{U} \in U(\mathbb{N})$ satisfying $\mathcal{U} \oplus \mathcal{U} = \mathcal{U}$ is called *idempotent*.

We can now describe the proof of Hindman's theorem. Let

$$X := \left\{ A \subseteq \mathbb{N} : \sum\nolimits_B \subseteq A \text{ for some infinite } B \subseteq A \right\}.$$

A simple argument (Proposition 4.1) will show that every idempotent ultrafilter is a subset of X. In particular, there exists an ultrafilter $\mathcal{F} \subseteq X$. Since $\mathbb{N} \in \mathcal{F}$ by property (1) above, and $\mathbb{N}$ is the disjoint union of finitely many sets (corresponding to the different colors), property (2) guarantees that one of these sets must be an element of $\mathcal{F}$. It follows that one of the elements of X is monochromatic, which is precisely the assertion of Hindman's theorem.

Actually, there is one small detail we've conveniently left undiscussed: the definition of the operation $\oplus$ on $U(\mathbb{N})$. This definition, given in (3.1), is somewhat opaque, and it's not even obvious *a priori* whether idempotent ultrafilters exist. Fortunately, a clever application of Zorn's lemma (Theorem 3.1) will resolve the issue.

2. Ultrafilters

As mentioned above, an ultrafilter on a set X can be viewed as the collection of all 'large' subsets of X. This seems innocuous enough; for example, if $X = [0,1]$, it might be reasonable to call a subset of X 'large' if it has measure 1. For many choices of X, however, the notion of measure might not be so readily available, making it difficult to ascertain whether any given set is large or not. This is why we instead consider the collection of all large subsets of X – that way, we only need to identify how large sets interact with each other, rather than properties of the individual subsets of X.

There is one set which is clearly large: X itself. Similarly, the empty set is small. What else can we say? Motivated by the example of the unit interval, it seems reasonable to assert that the intersection of any two large sets is still large. Finally, if a set A contains a large set, then A itself must be large. Formally:

Definition 2.1. *A collection $\mathcal{F}$ of subsets of X is a* filter *on X if*

(1) *$\emptyset \notin \mathcal{F}$ and $X \in \mathcal{F}$;*
(2) *if $A, B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$; and*
(3) *if $A \supseteq B$ and $B \in \mathcal{F}$, then $A \in \mathcal{F}$.*

An ultrafilter *on X is any maximal filter.*

By Zorn's lemma, one can show that any filter can be extended to an ultrafilter (although this extension is not necessarily unique).

Henceforth, we will work with ultrafilters on $\mathbb{N}$, the set of positive integers.[1] The space $U(\mathbb{N})$ of all such ultrafilters is quite large, having cardinality $2^{\mathfrak{c}}$ (here $\mathfrak{c}$ denotes the cardinality of the continuum). There is a natural topology on $U(\mathbb{N})$, given by the basis of open sets $\{\mathcal{U} \in U(\mathbb{N}) : A \in \mathcal{U} \text{ for some } A \subseteq \mathbb{N}\}$. Alternatively, one can view $U(\mathbb{N})$ as the largest compactification[2] of $\mathbb{N}$ (under the discrete topology). More precisely, if $X \supseteq \mathbb{N}$ is compact, such that $\mathbb{N}$ is dense in X and such that every continuous map from $\mathbb{N}$ to a compact set Y can be lifted uniquely to a map from $U(\mathbb{N})$ to Y, then $X \simeq U(\mathbb{N})$.

One crucial property of ultrafilters on $\mathbb{N}$ is the following:

Proposition 2.2. *Suppose $\mathcal{F}$ is an ultrafilter on $\mathbb{N}$. Then for all $A \subseteq \mathbb{N}$, either $A \in \mathcal{F}$ or $A^c \in \mathcal{F}$ (where A^c is the complement of A).*

In fact, it turns out that this is equivalent to the maximality of a filter.

Although we implied that an ultrafilter was meant to capture what it means for a subset to be large, the above proposition already hints that ultrafilters measure

[1] It is convenient in this argument to adopt the convention that $0 \notin \mathbb{N}$.

[2] This is the famous *Stone-Čech* compactification.

largeness in a curious way. For example, either the set of even integers or the set of odd integers will be considered large, while its complement will not. Even worse, there are some ultrafilters which consider finite subsets to be large, viz.

$$\langle 3\rangle := \{A \subseteq \mathbb{N} : 3 \in A\}.$$

Fortunately, this type of pathology is rare:

Theorem 2.3. *If an ultrafilter $\mathcal{F}$ on $\mathbb{N}$ contains a finite set, then $\mathcal{F} = \langle n\rangle$ for some n.*

Ultrafilters of the form $\langle n\rangle$ are called *principal.* Since the principal ultrafilters on $\mathbb{N}$ are countable whereas the space $U(\mathbb{N})$ of all ultrafilters is not, it is clear that principal ultrafilters are very rare.

We now prove one of the properties we mentioned in our sketch of Hindman's theorem.

Proposition 2.4. *Given an ultrafilter $\mathcal{F} \in U(\mathbb{N})$. If $A \sqcup B \in \mathcal{F}$ then $A \in \mathcal{F}$ or $B \in \mathcal{F}$.*

Proof. Suppose $A \notin \mathcal{F}$. Then its complement $A^c \in \mathcal{F}$, whence

$$B = (A \sqcup B) \cap A^c \in \mathcal{F}. \qquad \square$$

We take this opportunity to mention a tantalizing open question. Is it true that

$$U(\mathbb{N})\backslash\mathbb{N} \simeq U(\omega_1)\backslash\omega_1,$$

where we are removing the set of principal ultrafilters on both sides and ω_1 denotes the least uncountable ordinal? The answer is obviously no; however, no one has any idea of how to prove this.

3. Idempotent ultrafilters

We now define a binary operation $\oplus$ on $U(\mathbb{N})$ which is well-defined and associative, thus making $U(\mathbb{N})$ into a semigroup. For any $\mathcal{U}, \mathcal{V} \in U(\mathbb{N})$, set

$$\mathcal{U} \oplus \mathcal{V} := \Big\{A \subseteq \mathbb{N} : \{k \in \mathbb{N} : A - k \in \mathcal{U}\} \in \mathcal{V}\Big\} \tag{3.1}$$

where $A - k$ denotes the set $\{a - k : a \in A\}$. Note that $\oplus$ is not commutative on $U(\mathbb{N})$! However, it behaves very well on the set of principal ultrafilters. For example, it is a good exercise to prove that $\langle 3\rangle \oplus \langle 5\rangle = \langle 8\rangle$.

Recall from above that an ultrafilter $\mathcal{U} \in U(\mathbb{N})$ is called *idempotent* if $\mathcal{U} \oplus \mathcal{U} = \mathcal{U}$. In particular, none of the principal ultrafilters $\langle n\rangle$ are idempotent.[3] This raises the important question: do any idempotent ultrafilters exist?

[3] This property is the main reason we follow the convention that $\mathbb{N}$ does not include 0.

Theorem 3.1. *Idempotent ultrafilters exist.*

Proof. Let

$$\mathbb{A} := \{A \subseteq U(\mathbb{N}) : A \text{ is nonempty, closed, and } A \oplus A \subseteq A.\}$$

Note that $U(\mathbb{N}) \in \mathbb{A}$, and that any descending chain has nonempty intersection (since every $A \in \mathbb{A}$ must be compact). We may thus apply Zorn's lemma to deduce the existence of a nonempty minimal set $B \in \mathbb{A}$. We claim that *every* element of B is idempotent.

Since $B \in \mathbb{A}$ have $\mathcal{U} \oplus B \subseteq B$ for all $\mathcal{U} \in B$; minimality implies that $\mathcal{U} \oplus B = B$ for every $\mathcal{U} \in B$. It follows that for any $\mathcal{U} \in B$, there exists a $\mathcal{V} \in B$ such that $\mathcal{U} \oplus \mathcal{V} = \mathcal{U}$. Fix any $\mathcal{U} \in B$, and set

$$\widetilde{B} := \{\mathcal{W} \in B : \mathcal{U} \oplus \mathcal{W} = \mathcal{U}\}.$$

We now show that $\widetilde{B} \in \mathbb{A}$. By construction, we know $\widetilde{B} \neq \emptyset$. Further, it is closed, since it is a preimage of $\mathcal{U}$ under a shift by $\mathcal{U}$. Finally, one checks directly from the definition that $\widetilde{B} \oplus \widetilde{B} \subseteq \widetilde{B}$. It follows that $\widetilde{B} \in \mathbb{A}$. Since B is the minimal element of $\mathbb{A}$ and $\widetilde{B} \subseteq B$, we conclude that $\widetilde{B} = B$. In particular, this implies that $\mathcal{U} \oplus \mathcal{U} = \mathcal{U}$, i.e. that $\mathcal{U}$ is idempotent. Since $\mathcal{U}$ was an arbitrary element of the nonempty set B, the theorem is proved. □

4. Proof of Hindman's theorem

Having shown above the existence of idempotent ultrafilters on $\mathbb{N}$, we can now complete the proof of Hindman's theorem. Recall from the introduction the set

$$X := \left\{A \subseteq \mathbb{N} : \sum\nolimits_B \subseteq A \text{ for some infinite } B \subseteq A\right\}.$$

Proposition 4.1. *If $\mathcal{U} \in U(\mathbb{N})$ is idempotent, then $\mathcal{U} \subseteq X$.*

Proof. Fix any idempotent ultrafilter $\mathcal{U} \in U(\mathbb{N})$. For $A \in \mathcal{U}$, define

$$A^* := \{k \in \mathbb{N} : A - k \in \mathcal{U}\}.$$

If $A \in \mathcal{U}$, then $A \in \mathcal{U} \oplus \mathcal{U}$ (since $\mathcal{U}$ is idempotent), whence $A^* \in \mathcal{U}$. This implies that $A \cap A^* \in \mathcal{U}$, and hence, that $A \cap A^* \neq \emptyset$. Actually, we can say more: since the only ultrafilters containing finite sets are the principal ones, and idempotents cannot be principal, $A \cap A^*$ must be an infinite set.

Suppose $A \in \mathcal{U}$; we wish to show that $A \in X$. Let $A_0 = A$, and pick any $k_0 \in A_0 \cap A_0^*$. Now set

$$A_1 := (A_0 - k_0) \cap A_0;$$

this is an element of $\mathcal{U}$, by construction, and is thus nonempty. Moreover, $A_1 \cap A_1^* \in \mathcal{U}$, and is therefore an infinite set, so we can choose $k_1 \in A_1 \cap A_1^*$ which is larger than k_0.

We proceed in the same way, at each stage picking $k_n \in A_n \cap A_n^*$ such that $k_n > k_{n-1}$ (which we can do since $A_n \cap A_n^*$ is infinite) and setting

$$A_{n+1} := (A_n - k_n) \cap A_n.$$

Finally, let $B := \{k_n\}$. Since the sequence k_n is strictly increasing, B is an infinite set. An easy induction argument shows that for any finite set of indices I,

$$\sum_{i \in I} k_i \in A_{\inf I}.$$

It follows that $\sum_B \in A$, whence $A \in X$. □

Department of Mathematics, University of Toronto
40 St. George Street, Room 6290
Toronto, M5S 2E4, Canada
E-mail address: leo.goldmakher@utoronto.ca