

REU'09·Transfinite combinatorics·Lecture 9

Instructor: László Babai

Scribe: Thomas Church

July 31, 2009

9.1 Ultraintegers: Exponentiation and factoring

Take \mathbb{N} with $(+, \cdot, 0, 1)$. Can we find a sentence expressing exponentiation?

$$\varphi(x, y, z): z = x^y$$

We saw that for the ultrapower $\mathbb{N}^* = \mathbb{N}^{\aleph_0} / \mu$, sentences involving exponentiation usually translated (e.g. Fermat's little Theorem).

How about the Fundamental Theorem of Arithmetic? (Namely, every number can be expressed uniquely as a product of primes.) Consider some examples of ultraintegers:

The only (ultra)prime that divides the ultrainteger $[1, 2, 4, 8, 16, \dots]$ is $\underline{2} = [2, 2, 2, \dots]$. What should the exponent be?

$$[1, 2, 4, 8, 16, \dots] = \underline{2}^{[0, 1, 2, 3, \dots]}$$

Now let p_1, p_2, \dots be distinct primes, and consider $\underline{p} = [p_1, p_1 p_2, p_1 p_2 p_3, \dots]$. This is divisible by $\underline{p}_1 = [p_1, p_1, p_1, \dots]$, by \underline{p}_2 , by \underline{p}_3 , etc. But it is also divisible by the prime $[p_1, p_2, p_3, \dots]$. Also by the distinct prime $[0, p_1, p_2, p_3, \dots]$. Also by the distinct prime $\underline{p} = [p_1, p_1, p_2, p_2, \dots]$. So how many prime divisors does \underline{p} have? We know it is at most 2^{\aleph_0} , since this is the cardinality of \mathbb{N}^* . (Proof: we find equal lower and upper bounds:

$$2^{\aleph_0} \leq \aleph_0^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}.)$$

Exercise 9.1. Prove that \underline{p} has 2^{\aleph_0} distinct prime divisors. (Hint: embed binary tree into sets of prime divisors.)

We want to say that unique prime factorization is true over \mathbb{N}^* , but the number of prime factors should be an ultrainteger. Perhaps we want

$$z = \prod_{i=1}^s \underline{p}_i^{k_i}$$

to be defined by

$$z(j) = \prod_{i(j)=1}^{s(j)} p(j)_{i(j)}^{k(j)_{i(j)}}$$

Exercise 9.2. Check this definition. Verify unique prime factorization of ultraintegers.

We shall now take another route to proving that unique prime factorization holds among ultraintegers: we shall show that the Fundamental Theorem of Arithmetic is a first-order sentence.

Exercise 9.3. Lemma: for any sequence a_0, \dots, a_n of nonnegative integers there exist b, c such that for each $0 \leq i \leq n$, $\text{rem}(c, b+i) = a_i$. Here $\text{rem}(r, s)$ is the remainder when dividing r by s (defined by the property that $r \equiv \text{rem}(r, s) \pmod s$ and $0 \leq \text{rem}(r, s) < s$).

This says that we can encode an arbitrary sequence a_0, \dots, a_n into just three integers b, c, n . (Note that one can easily encode (b, c, n) by a single integer; this will give a slight variation on Gödel's numbering scheme.)

Now we can encode the sequence $1, x, x^2, x^3, \dots, x^y$. The following sentence recognizes the encoding of this sequence:

$$\text{rem}(b, c) = 1 \wedge (\forall i)(1 \leq i \leq y \rightarrow \text{rem}(c, b+i) = x \cdot \text{rem}(c, b+i-1) \wedge \text{rem}(c, b) = 1).$$

Thus we have

$$\begin{aligned} x^y = z &\iff (\exists b, c) \\ &[(\forall i)(1 \leq i \leq y \rightarrow \text{rem}(c, b+i) = x \cdot \text{rem}(c, b+i-1) \\ &\quad \wedge \text{rem}(c, b) = 1 \wedge \text{rem}(c, b+y) = z)] \end{aligned}$$

Exercise 9.4. Show that the Fundamental Theorem of Arithmetic is expressible as a first-order sentence (over \mathbb{N}).

9.2 Ramsey theory, large cardinals

From last time, Ramsey's theorem (infinite version, special case): $\aleph_0 \rightarrow (\aleph_0, \aleph_0)$. With ultrafilters: fix an ultrafilter on the set of vertices. Color each vertex red or blue according to whether almost all of its edges are red or almost all of its edges are blue. Now almost all vertices are red or almost all are blue; assume the former, and consider the red vertices. Pick one to be v_1 ; almost all vertices are connected to v_1 by a red edge, so choose one of these to be v_2 . Now almost all vertices are connected to v_1 and to v_2 by a red edge, so choose one of these to be v_3 . Continue to obtain an infinite red clique.

Without ultrafilters, we proceed as follows. We construct a sequence of vertices v_i so that for each i , all the edges (v_i, v_j) for $j > i$ are of the same color. Having done this, color each v_i by the color of all of those edges; then the collection of all red v_i is a red clique, and the collection of all blue v_i is a blue clique. At least one of these cliques is infinite.

(To construct this sequence, choose any v_1 ; it has infinitely many edges of one color, say red. So throw out all the vertices not connected by a red edge to v_1 , and choose an arbitrary remaining vertex to be v_2 . It has infinitely many edges of one color, so throw out all remaining vertices not connected to v_2 by a edge of that color, and choose an arbitrary remaining vertex to be v_3 ...)

Exercise 9.5 (Ramsey's Theorem, finite version, special case).

$$A : \aleph_0 \rightarrow (\aleph_0, \aleph_0)$$

$$B : (\forall k, \ell)(\exists N)(N \rightarrow (k, \ell))$$

Prove $A \implies B$.

Exercise 9.6. • $6 \rightarrow (3, 3)$

• $17 \rightarrow (3, 3, 3)$

• $\aleph_0 \rightarrow (\aleph_0, \aleph_0, \aleph_0)$

Exercise from last time: $2^{\aleph_0} \not\rightarrow (\aleph_0, \aleph_0)$; that is, there exists a coloring of the edges of the complete graph on 2^{\aleph_0} vertices such that every red clique, and every blue clique, is countable.

Lemma 9.7 (From last time). Any well-ordered subset of \mathbb{R} (with its usual ordering) is countable.

We have $(\mathbb{R}, <)$ with its usual ordering; we may also take a well-ordering (\mathbb{R}, \prec) .

Now define a coloring on the complete graph $K_{\mathbb{R}}$ by saying that the edge from x to y is red if the orderings agree:

$$x < y \wedge x \prec y \quad \text{or} \quad x > y \wedge x \succ y$$

and blue otherwise. Now any red clique is a well-ordered subset, and thus by the lemma is countable. Applying the lemma to the reverse ordering shows the same holds for blue cliques.

Exercise 9.8. Prove that $2^{\mathfrak{m}} \not\rightarrow (\mathfrak{m}^+, \mathfrak{m}^+)$, where \mathfrak{m}^+ is the successor of cardinal \mathfrak{m} . (I. e., if $\mathfrak{m} = \aleph_\alpha$, $\mathfrak{m}^+ = \aleph_{\alpha+1}$.)

Definition 9.9. \mathfrak{m} is *strongly inaccessible* if

1. \mathfrak{m} is not the sum of fewer, smaller cardinals
2. $(\forall \kappa)(\kappa < \mathfrak{m} \implies 2^\kappa < \mathfrak{m})$

Exercise 9.10. Verify that \aleph_ω violates (1.), because

$$\aleph_\omega = \sup_{\kappa < \omega} \aleph_\kappa = \sum_{\kappa < \omega} \aleph_\kappa$$

Exercise 9.11. If $\mathfrak{m} \rightarrow (\mathfrak{m}, \mathfrak{m})$, then \mathfrak{m} is strongly inaccessible.

Exercise 9.12. If \mathfrak{m} is strongly inaccessible and $\mathfrak{m} = \aleph_\alpha$, then $|\alpha| = \mathfrak{m}$.

Exercise 9.13. Let \mathfrak{m} be the smallest cardinal such that a countably additive $(0, 1)$ -measure on \mathfrak{m} exists. Then $\mathfrak{m} \rightarrow (\mathfrak{m}, \mathfrak{m})$.