REU'09·Transfinite combinatorics·Lecture 8

Instructor: László Babai
Scribe: Thomas Church

July 29, 2009

8.1 Ultra-integers

Take $\mathbb{N}$ with $(+, \cdot, 0, 1, <)$. Form the ultrapower $\mathbb{N}^* = \mathbb{N}^{\aleph_0}/\mu$.

Definition 8.1. Divisibility: $\underline{x} \mid \underline{y}$ if

$$\exists \underline{z} \colon \underline{x}\,\underline{z} = \underline{y}.$$

This is equivalent to: for almost all i, $x(i) \mid y(i)$.

Definition 8.2. Prime numbers: p is prime if $p \neq 1$ and $(d \mid p \implies d = 1$ or $d = p)$.

Thus $\underline{p}$ is prime $\iff$ for almost all i, $p(i)$ is prime.

Goldbach's conjecture. If $n \geq 4$, n even, then $\exists$ primes p_1, p_2 such that $n = p_1 + p_2$.

An even ultrainteger is one which is almost always even; it is $\geq \underline{4}$ if it is almost always ≥ 4. Thus assuming Goldbach's conjecture, if $\underline{n} \geq 4$ and $\underline{n}$ is even, then for almost all i, $\underline{n}(i) = \underline{p}_1(i) + \underline{p}_2(i)$; this defines prime ultraintegers $\underline{p}_1$ and $\underline{p}_2$.

Shorter proof: Goldbach's conjecture is a first-order statement, so it is true in $\mathbb{N}^* \iff$ it is true in $\mathbb{N}$.

Fermat's Last Theorem. $(\forall x, y, z, n)(n \geq 3 \wedge x^n + y^n = z^n) \to (xyz = 0)$

Exercise 8.3. Prove that replacing the equality above with $x^n + y^n + z^n = 0$, where now x, y, z range over all integers (not just nonnegative integers) is equivalent to the usual statement of FLT.

Since FLT is true in $\mathbb{N}$, it is also true in $\mathbb{N}^*$: a counterexample $\underline{x}, \underline{y}, \underline{z}, \underline{n}$ such that $\underline{x}^{\underline{n}} + \underline{y}^{\underline{n}} = \underline{z}^{\underline{n}}$, would consist of infinitely many counterexamples to FLT, one for almost every i.

Fermat's Little Theorem. p prime, x integer $\implies p \mid (x^p - x)$.

Also true for ultra-integers.

Certainly $\underline{p} = (2, 3, 5, 7, 11, \ldots)$ is prime. How about $\underline{p}' = (11, 17, 23, 29, \mathbf{35}, \ldots,)$?

Theorem 8.4 (Dirichlet's theorem)**.** Any infinite arithmetic progression in which the terms and the increment are relatively prime contains infinitely many primes.

Exercise 8.5. Prove that every non-constant infinite arithmetic progression contains an infinite number of composite numbers.

Exercise 8.6. Let $\underline{p}'$ be the equivalence class of an arithmetic progression in which the terms are relatively prime to the increment. Prove: whether or not $\underline{p}'$ is an ultra-prime depends on the ultrafilter.

Theorem 8.7 (4 squares theorem)**.** $(\forall x)(\exists y_1, \ldots, y_4)(x = y_1^2 + \cdots + y_4^2)$

Are the ultraintegers well-ordered? $\omega^* \subset \left(\omega^{\aleph_0}/\mu\right)$? Is there an infinite decreasing sequence of ultraintegers?

Infinitely large ultraintegers: the ordinary integers in $\mathbb{N}^*$ are e.g. $(7, 7, 7, \ldots)$. The ultrainteger $(0, 1, 2, 3, \ldots) > (9, 9, 9, 9, \ldots)$, since the former is almost always greater than the latter.

Now $(0, 1, 2, 3, \ldots)$"-1"$=(0, 0, 1, 2, \ldots)$ is less than $(0, 1, 2, 3, \ldots)$, since the former is always less than the latter. Iterating this, we obtain an infinite decreasing sequence of ultraintegers. Thus $\mathbb{N}^*$ is not well-ordered; this implies that well-ordered-ness is not a first-order property.

Exercise 8.8. Look up the definition of "solvable group". Is "solvable group" elementary? Is "non-solvable group" elementary?

Consider the property of a set being infinite, or of being finite. Which of these are elementary?

Well, to express "$|A| = \infty$", we want sentences P_n so that $P_n \iff |A| \geq n$; we may choose

$$P_n : \quad (\exists x_1, \ldots, x_n)\Big(\bigwedge_{i<j} x_i \neq x_j\Big)$$

Thus infinite-ness is elementary. Can finite-ness be elementary? No: consider the ultraproduct of finite sets of increasing size. If "this set is finite" could be expressed with a first-order sentence, then it would be true of the ultraproduct as well, but the ultraproduct is infinite.

8.2 Completeness, categoricity

- complete theory (set of sentences): Σ is complete if for every sentence φ, either $\Sigma \implies \varphi$ or $\Sigma \implies \neg\varphi$.

  (We say that $\Sigma \implies \varphi$ if for any model $\mathcal{A} \models \Sigma$, $\mathcal{A} \models \varphi$. This was previously written $\Sigma \models \varphi$.)

- categorical in cardinality $\mathfrak{m}$: there is a unique model of cardinality $\mathfrak{m}$.

Theorem 8.9 (Tarski-Vaught principle, incorrect)**.** If Σ has an infinite model and Σ is categorical in some infinite cardinal $\mathfrak{m}$ then Σ is complete.

Proof. (attempt) Let $\mathcal{A} \models \Sigma$ be the unique model of cardinality m. Given a sentence φ, exactly one of φ and $\neg\varphi$ is true in $\mathcal{A}$, WLOG $\mathcal{A} \models \varphi$. We want to show that $\Sigma \implies \varphi$; that is, φ is true in all models of Σ.

Suppose not, so $\Sigma \not\Longrightarrow \varphi$. Then there exists a model $\mathcal{B} \models \Sigma$ where φ is not true: $\mathcal{B} \models \neg\varphi$.

Combining upward and downward Lowenheim-Skolem theorems, for every infinite cardinality ν, $\exists \mathcal{B}'$ elementary equivalent to $\mathcal{B}$ with cardinality $|\mathcal{B}'| = \nu$. In particular, we may choose $\mathcal{B}'$ to have cardinality m. Then $\mathcal{B}'$ is isomorphic to $\mathcal{A}$, while $\mathcal{A} \models \varphi$ and $\mathcal{B}' \models \neg\varphi$; this is a contradiction. $\square$

The flaw in the proof is that just because we have a model $\mathcal{B} \models \neg\varphi$, we don't know that there exists an *infinite* such model. Counterexamples are easy to construct: consider the empty theory on the empty language, or less trivially, consider the theory of complete graphs. The sentence $P_7 : (\exists x_1, \ldots, x_7)(\bigwedge x_i \neq x_j)$ is satisfied by any infinite model; but any model of cardinality ≤ 6 will satisfy $\neg P_7$. This may seem unsatisfying, since only six models give us any trouble; but recall that if we had models for $\Sigma \cup \{\neg\varphi\}$ of arbitrarily large finite cardinality, we could apply ultraproducts to construct an infinite model for $\Sigma \cup \{\neg\varphi\}$. This would be a contradiction, by the argument above.

This shows that any theory with both finite and infinite models cannot be complete. To fix this, we make the following change:

Theorem 8.10 (Tarski-Vaught principle, corrected)**.** If Σ has an infinite model and Σ is categorical in some infinite cardinal $\mathfrak{m}$ then $\Sigma \cup \{P_n : n \in \omega\}$ is complete. (Equivalently, we could require that Σ has no finite models.)

Exercise 8.11. (Fagin's Theorem) A first-order sentence about graphs is either true for almost all finite graphs, or false for almost all finite graphs. We proved this using the Tarski-Vaught principle, using the fact that the theory of "the random graph" is categorical in $\aleph_0$. Revisit our argument, with the revised Tarski-Vaught principle in mind.

8.3 Well-ordered subsets of $\mathbb{R}$

Exercise 8.12. Prove that every well-ordered subset of $\mathbb{R}$ (with its usual ordering) is countable.

Exercise 8.13 (Lemma)**.** Any collection of disjoint intervals in $\mathbb{R}$ is countable.

Now to prove Ex. 8.12, take a well-ordered subset X of $\mathbb{R}$. For each $x \in X$, let x^+ be the successor of x in X (or $x^+ = \infty$ if $x = \max X$). Then for each x, we take the open interval (x, x^+). This collection is disjoint, so by the lemma, X is countable.

8.4 Transfinite Ramsey theory

Exercise 8.14. Prove $\aleph_0 \to (\aleph_0, \aleph_0)$. This means: If you take an infinite complete graph, and color every edge either red or blue, then there will either be an infinite red clique (complete subgraph with only red edges) or an infinite blue clique.

Exercise 8.15. Prove: $2^{\aleph_0} \not\to (\aleph_1, \aleph_1)$. This means: There exists a red-blue coloring of the complete graph on $2^{\aleph_0}$ vertices such that every red clique and every blue clique is countable.