

Outline for Lecture 5

Joe Kilian

September 26, 2006

1. Quantified polynomial identities over natural numbers

(a) Definition

- Example: Fermat's last theorem for $n=3$
- Multiple quantifiers

(b) Strategy

- Post Correspondence Problem
- Express in terms of quantifiers, concatenation, etc.
- Convert to numbers - with lots of enhanced features
- Get rid of enhancements

(c) Express in terms of quantifiers

- $tval, bval$
- shrinking giant concatenation with array values, $tTOTAL, bTOTAL, CHOICE$
- note weird quantifiers

(d) Express in terms of numbers

- adding $tshift, bshift$

(e) Simplifying I

- Expressing $tval, bval, tshift, bshift$ as polynomials
- Expressing $<, =, >$
- Expressing AND OR

(f) Simplifying II

- Chinese Remaindering
- Expressing vectors as mods
- Expressing mods

2. Nontriviality Problem for Probabilistic Finite Automata

(a) Review

- Configurations of 2Counting Machines
- Termination is a sequence of near-equality assertion

- Rephrasing context-free language result
 - Properties of the “elimination game”
- (b) Dealing with multiple near-equalities
- Result of Scoring Game
 - Repeating trick

3. Characterization for RE Sets, Arithmetic Hierarchy

- (a) $RE = \exists y D(< x, y >)$
- (b) Reduction to Halting Problem
- (c) How to tell if D always halts?
- (d) Always halt if in $\forall\exists$.
- (e) Can we eliminate quantifiers?
- (f) SuperHalt: Halt with a Halt oracle
- (g) SuperHalt is in $\exists\forall$.