Some Open Problems in Proof Complexity

Paul Beame

University of Washington

Random Formulas

- Show that random formulas are hard for
  - cutting planes
  - depth 2 Frege
    - **Problem:** for **AC^0-Frege** all we know is the restriction method but restriction families seem to almost certainly falsify random formulas

- **Conjecture:** Random formulas are hard for Frege

Weak Pigeonhole Principle

- Prove hard: $PHP^{m \to n}$ for $\mathbf{m} >> \mathbf{n}$, e.g. $\mathbf{m=2^{n^{\epsilon}}}$
  - Has **quasi-**polynomial size depth 2 Frege proofs for $\mathbf{m} \geq \mathbf{(1+\epsilon)n}$
  - Lower bounds for resolution only non-trivial when $\mathbf{m < n^2/\log n}$
  - applications to bounded arithmetic (existence of infinitly many primes) and provability of $\mathbf{NP \not\subset P/poly}$

Lovasz-Schrijver Proof Systems

- Like cutting planes but based on 01-programming:
  - Initial inequalities and goal like cutting planes
    - Plus $x^2=x$ substitution
    - No division rule
  - Can create non-negative degree two polynomials by
    - multiplying two non-negative linear quantities or
    - squaring any linear quantity
  - Polynomially simulates resolution; proves **PHP**
- Has feasible interpolation so given **NP**$\not\subset$**P/poly** not polynomially bounded but no known hard tautology
  - Is **Count**$^{\mathbf{2n+1|2}}$ hard for them?

The bigger questions

- Prove lower bounds for **AC^0[p]-Frege**
  - Show **Count$^{qn+1|q}$** hard?

- Prove lower bounds for **TC^0-Frege/Frege**
  - Several candidates, e.g. **AB=I Þ BA=I** for Boolean matrix multiplication

Proof search for PCR

- Can we build better algorithms to beat the Davis-Putnam/DLL algorithms in practice by using some PCR ideas?

See also

- http://www.cs.washington.edu/homes/beame/papers/eatcs-survey.ps