**RANOMIZED COMPUTATION NETWORKS**

The ASPLOS "Wild and Crazy Ideas" Session
Rick Hangartner

**WHY RANDOMIZED ALGORITHMS?**

- Fastest and most elegant algorithms for many real problems
  - Equivalence of OBDDs: Blum et al. - IPL 1980
- BPP achievable with imperfect random sources
- At best, derandomization algorithms non-uniform
- Conjectured BQP contains no interesting problems outside BPP
  - Fortnow & Rogers - preprint 1997
  - Cambridge University Press

**RANDOMIZED COMPLEXITY CLASSES AND ALGORITHMS**

- Monte Carlo (2-sided)
  - \( p(\text{YES/YES}) \to 1 \)
  - \( p(\text{NO/NO}) \to 1 \)
  - \( p(\text{no answer}) = 0 \)
- Monte Carlo (1-sided)
  - \( p(\text{YES/YES}) = 1 \)
  - \( p(\text{NO/NO}) \to 1 \)
  - \( p(\text{no answer}) = 0 \)
- Las Vegas
  - \( p(\text{YES/YES}) = 1 \)
  - \( p(\text{NO/NO}) = 1 \)
  - \( p(\text{no answer}) = 0 \)

**RCN AS RAM REPLACEMENT**

- Results RAM
- Connection RAM
- Configurable Logic
- Test Logic
- Random Bit Register
**GENERIC RCN ARCHITECTURE**

- RAM cell
- Connection RAM
- Buffer
- Flip Latch
- Random Bit Register
- Results RAM
- Expansion Interface

**RANDOM BIT GENERATORS**

- Direct Coupled
- Capacitively Coupled

**DYNAMICAL SYSTEMS MODEL**

- SAT Instance
- Connection RAM
- Random Bit Register

- System Noise

- DNF expressions (coRP)
- Decides equivalence of DNF expressions (coRP)
- Realizes Blum et.al. algorithm for deciding equivalence of generalized BDDs

- Operations over an algebraic field with at least 2k elements

- k-vector of log 2k-bit random elements

- Product term (2k+1 bits)

- Fixed point is a solution!

- Make a random choice

- Unsatisfiable if $O(|x|^n)$ fails