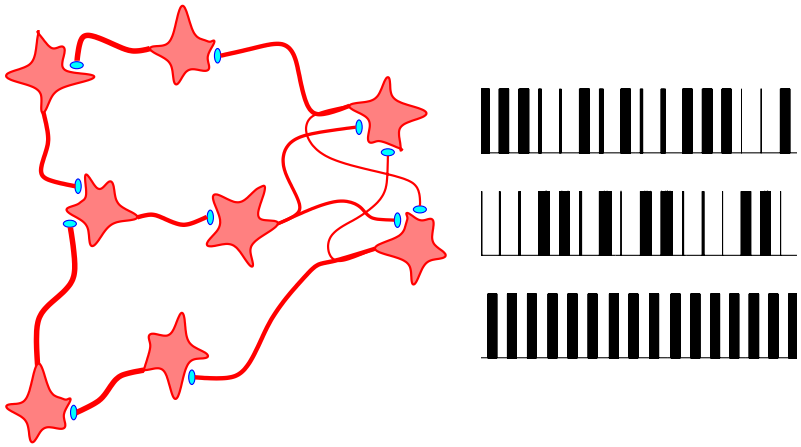
RANDOMIZED COMPUTATION NETWORKS



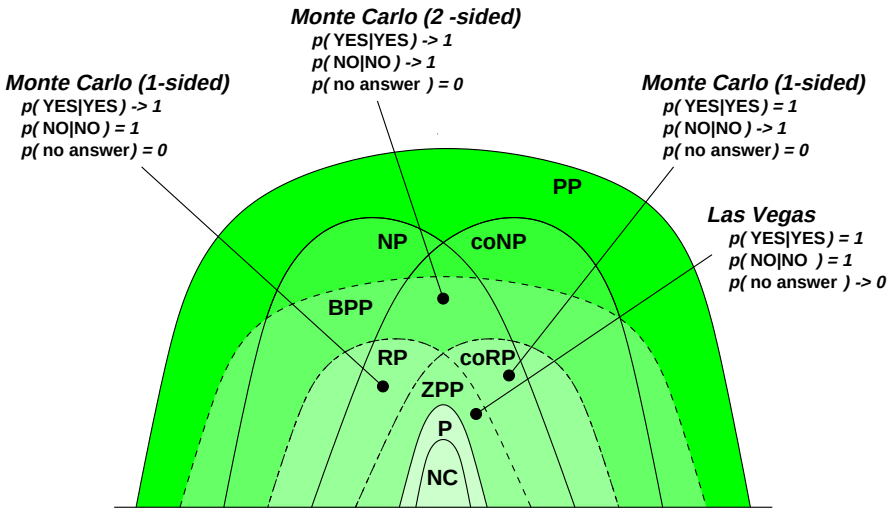
The ASPLOS "Wild and Crazy Ideas" Session

Rick Hangartner

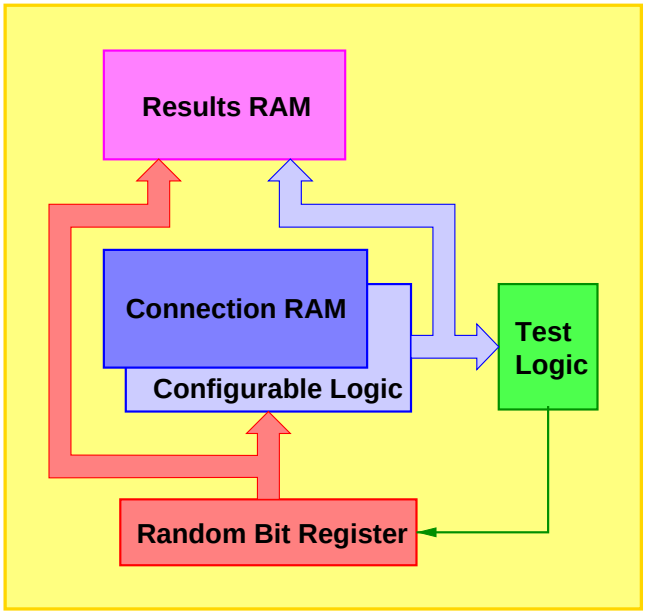
WHY RANDOMIZED ALGORITHMS?

- **Fastest and most elegant algorithms for many real problems**
  Primality Testing: Rabin - JNT 1980, Adleman & Huang - STOC 1987
  Equivalence of OBDDs: Blum et. al. - IPL 1980
- **BPP achievable with imperfect random sources**
  Zuckerman - FOCS 1991, Andreev et. al. - FOCS 1997
- **At best, derandomization algorithms non-uniform**
  Nisan & Wigderson -JCSS 1994, Andreev et. al. - JACM 1998
- **Conjectured BQP contains no interesting problems outside BPP**
  Fortnow & Rogers - preprint 1997
- ***Randomized Algorithms,*** **Motwani and Raghavan, 1996**
  Cambridge University Press

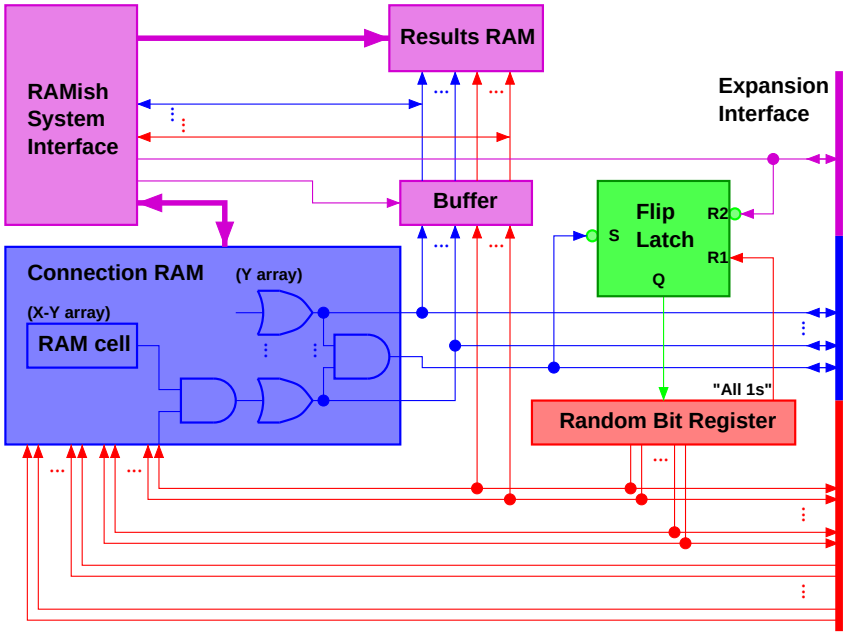
RANDOMIZED COMPLEXITY CLASSES AND ALGORITHMS



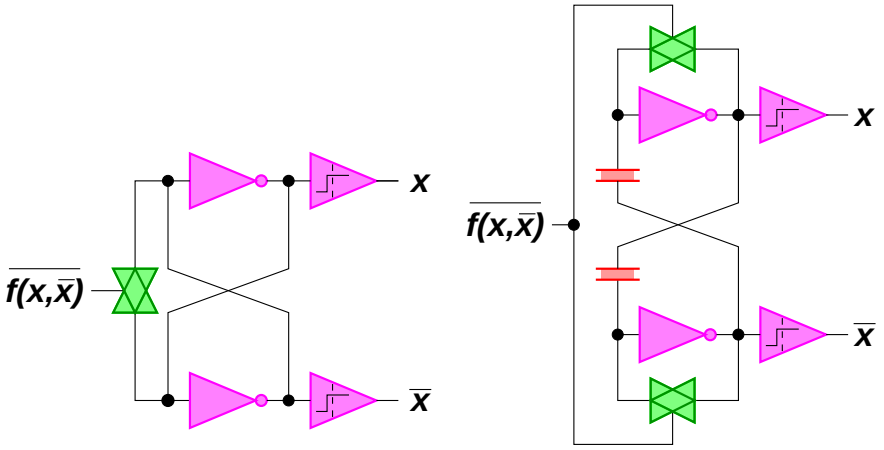
RCN AS RAM REPLACEMENT



GENERIC RCN ARCHITECTURE



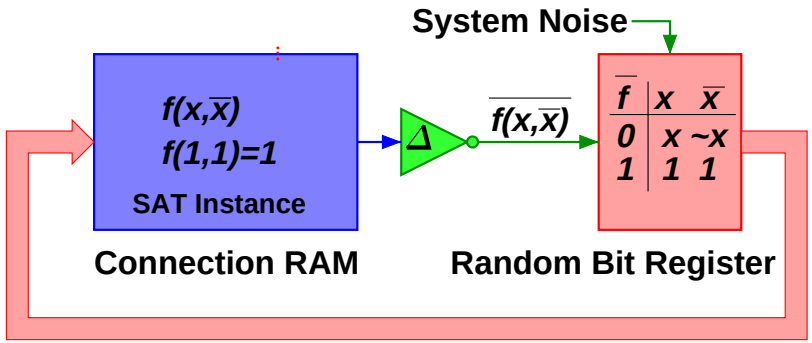
RANDOM BIT GENERATORS



Direct Coupled

Capacitively Coupled

DYNAMICAL SYSTEMS MODEL



f(x,x̄)=0 => x=1, x̄=1

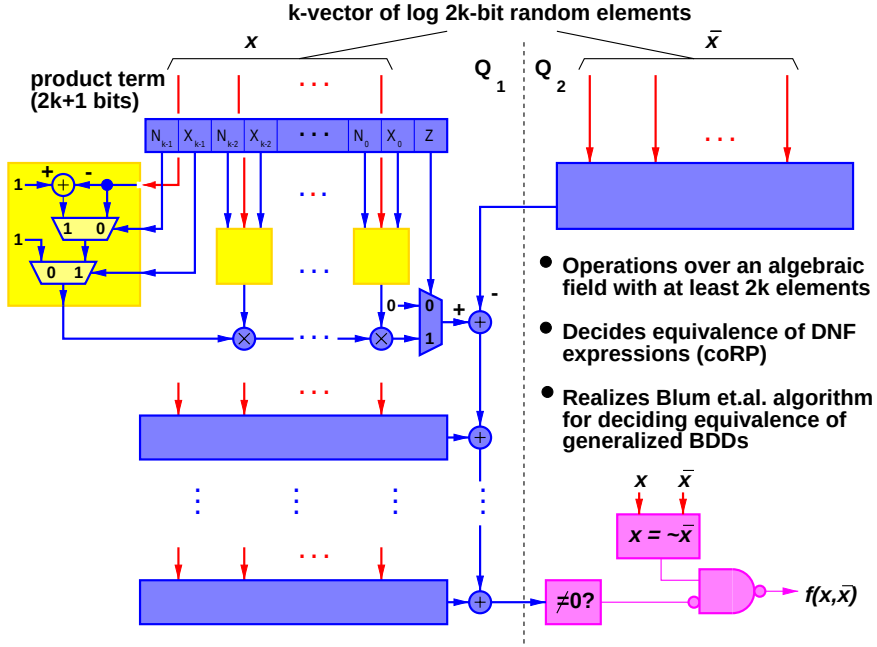
f(1,1)=1 => x=0/1, x̄=~x make a random choice

f(x,x̄)=0 => x=1, x̄=1 if not satisfying, repeat...

f(x,x̄)=1 => x=x, x̄=x̄ fixed point is a solution!

f(x,x̄)=0 => x=1, x̄=1 unsatisfiable if $O(|x|^n)$ fails

RCN FOR MULTINOMIAL EQUIVALENCE



- Operations over an algebraic field with at least 2k elements
- Decides equivalence of DNF expressions (coRP)
- Realizes Blum et.al. algorithm for deciding equivalence of generalized BDDs