RANDOMNESS AND APPROXIMATION

RJ Lipton
A Story

• Given a polynomial $f(x)$
  • Find its roots

• Polynomial time algorithm in degree $f(x)$

• But…
A Question

• Where does \( f(x) \) come from?
• The eigenvalues of real symmetric matrices

• All roots real
• Better methods to solve

\[
A = \begin{bmatrix}
3 & 1 & -1 \\
1 & 3 & -1 \\
-1 & -1 & 5
\end{bmatrix}
\]

\[
\text{det}(A - \lambda I) = \begin{bmatrix}
3-\lambda & 1 & -1 \\
1 & 3-\lambda & -1 \\
-1 & -1 & 5-\lambda
\end{bmatrix}
\]
The Point

• Moore’s Law Stops?

OCTOBER 22, 2014

IEEE panel agree Moore's Law via Lithography scaling will be dead by 2035 and explore Beyond CMOS

• Must get to core problems

• Perhaps use
  • Randomness
  • Approximation
Worst Case

Input

A

Output
Average

Input

Output
Random

Input

Output
Models

• Worst Case
  • For all inputs runs in time T

• Average Case
  • For most inputs runs in time T

• Random Case
  • For all inputs runs in time T with probability ≈1
Why Useful?

- Sampling
- Test properties
- Look at small part of information
- Others
Sampling

- Economy
- Weather
- Molecular
- Genetics
- Load balancing
  - Distributed sorting
Sampling
Testing

• Equality

\[12^{2000001} + 7^{46466} = 143^{10100101} + 198^{45546}\]?

• Expense

• Can do via randomness
Approximation

- Compute $f(x)$ or compute $g(x)$ so
  - Distance($f(x), g(x)$) is small

- Makes sense
  - Many problems
  - Not all
DFT

- Given N points can compute in order $N \log(N)$ operations
  - Any inputs
  - No randomness
Sparsity
Results

• On N points if k sparse
  • Order operations $k \log(N)$ random algorithm

• Approximate sparse

$$\|\text{result} - \hat{x}\|_2 \leq (1 + \epsilon) \min_{k\text{-sparse } \hat{x}_{(k)}} \|\hat{x}_{(k)} - x\|_2$$
Random Bit Generation

• Issues with generation of random bits

• “Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.”

• “Hard to generate…”
Random Bits

- Algorithms vary
  - Some use few
    - Crypto
  - Some use more
    - Hashing
- Some use lots
  - Sampling
  - Testing
Issues

• How create culture support random/approximate?

• Harder to debug and test?

• Change view of world?