Searching for the infamous Random Number Generator (RNG)

Luther Vucic

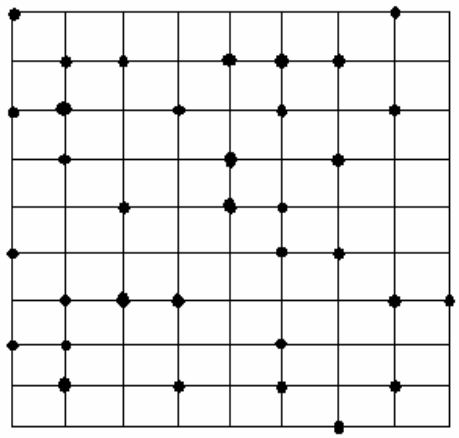
Advisor: Gary Reich

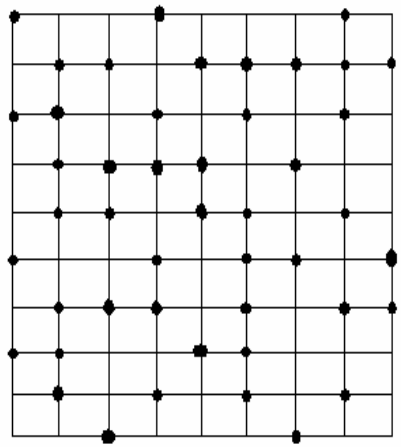
The Basis of
The larger picture

- Looking at general characteristics in Phase Transition
  - Phase transitions in properties such as magnetism and conduction
  - Find a successful model based on the geometry and structure of the atoms
  - Bonds between atoms do not affect the properties as much as the patterns that are form

Percolation Theory

- Percolation Theory
  - Lattice – structure
    - Finite vs Infinite
    - Square, Triangular, Honeycomb
  - Random points
    - Determine the filling pattern of lattice
  - Form clusters
    - Cluster is nearest neighbor
    - As number of points fill the clusters begin to merge to form larger clusters
    - Reach critical point then the cluster percolates





What is a RNG?

- A process that obtains a list of numbers with no known correlation. (Perfect RNG)
- Most RNG's are mathematical algorithms or observed random physical events
- Parts:
  - Process/Algorithm
  - Period
  - Correlations
  - Speed

Unbiased Tests Of Randomness

- Run Test
  - looks for runs in the numbers
- Runs below mean
  - same as above except that it focuses on under or above the mean value
- Equidistribution test
  - checks to make sure the numbers are equally distributed throughout
- Chi squared
  - compares a theoretical fit to an observed data

Domb's Contribution to Percolation Theory

- Found exact results of counts of clusters that would form finite lattice of (17,36) (cluster site, perimeter site)
- Able to calculate the probability of getting a site 'n' with a perimeter 's'

$$\Pr ob = n \times Domb \times p^{n-1} \times (1-p)^{s}$$

The RNG's

- Native- not really known how this algorithm is constructed
- Marsaglia/Zaman uses two RNG's then multiplies them to form one number
- Knuth is in the form of

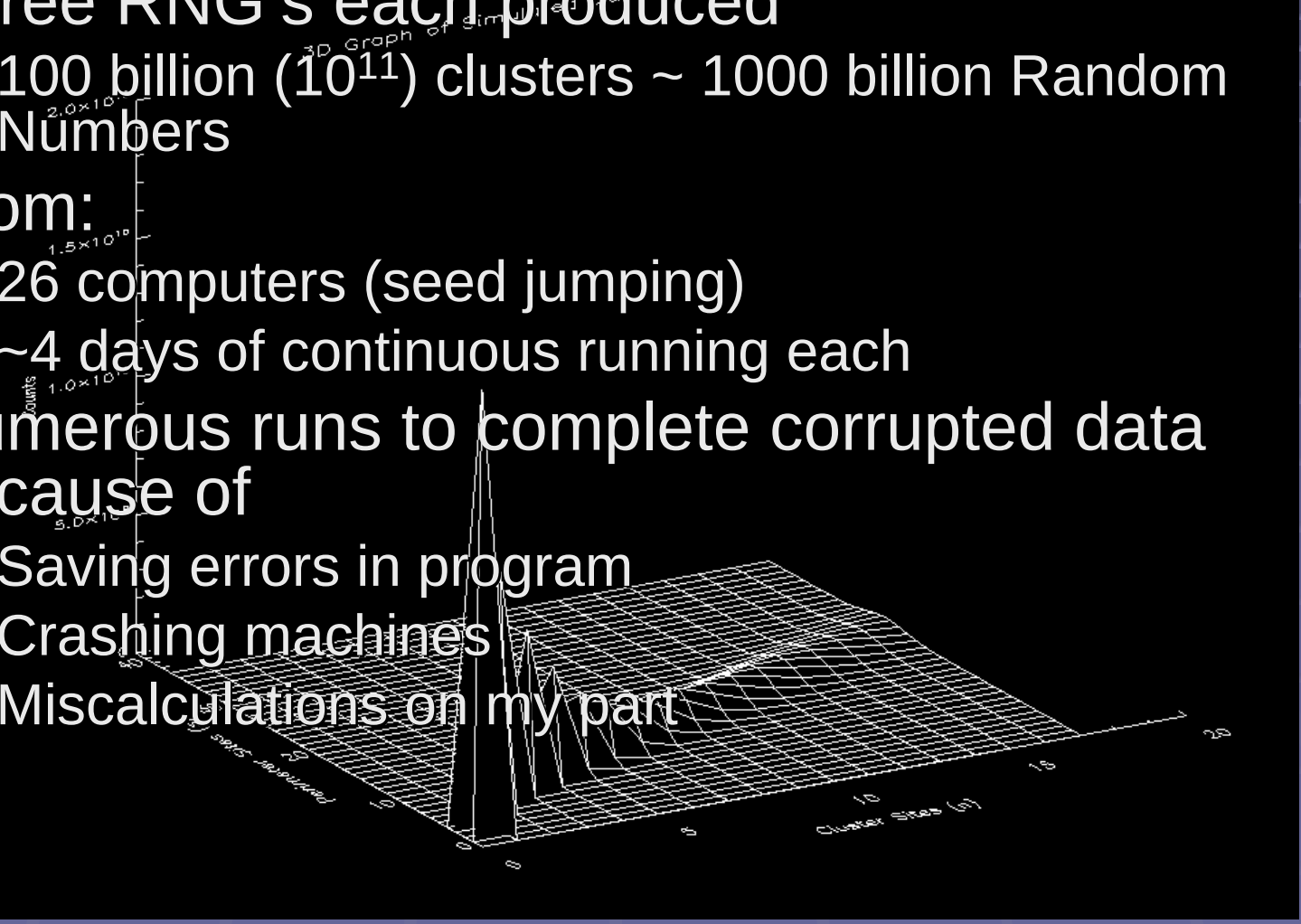
$$x = (ax + c) \bmod m$$

The Three Wise RNG's

RNG	IDL Native	Marsaglia and Zaman	Knuth's
Theory	Little theory	More theory	More theory
Speed	350s per billion	1800s per billion	590s per billion
Document	From Num Rec.	Well tested widely used	Claim good no data

Many Days Later
The Data is Finally Produced

- Three RNG's each produced
  - 100 billion (10^{11}) clusters ~ 1000 billion Random Numbers
- From:
  - 26 computers (seed jumping)
  - ~4 days of continuous running each
- Numerous runs to complete corrupted data because of
  - Saving errors in program
  - Crashing machines
  - Miscalculations on my part



Chi Squared Test

$$x^2 = \Sigma \frac{(y - n)^2}{n}$$

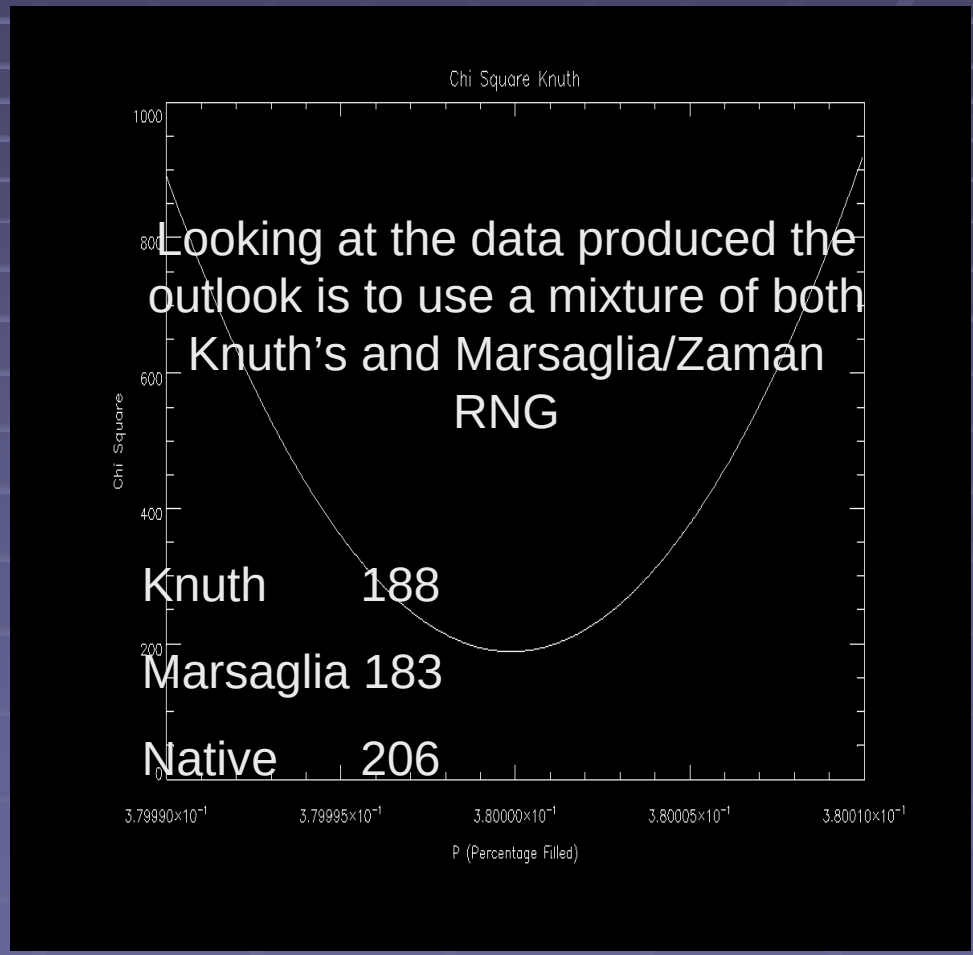
- Where
  - X^2 is the chi squared value
  - Y is the observed frequency
  - N is the theoretical frequency
- This is a test to determine the closeness of fit

Percentage	1%	5%	25%	50%	75%	95%	99%
X^2 value	140	151	168	180	194	213	228

Conclusions on the RNG

- Native produced a 91% less chi value
- Marsaglia/Zaman produced a 58 % less chi value
- Knuth produced a 75% less chi value

- Used the X^2 function in IDL to determine percentages



Outlook to Future Work

- Instituting the RNG into the actual Phase transition simulation
- Expanding Domb's work to larger Clusters
  - Focus on single size
  - Analyze shape and perimeter size

Acknowledgements

- Gary Reich
- Union Physics Department
- Union College Research Fellowship