Undergraduate Research
Mathematics and Computer Science

Jeff Kinne

Panel on Undergraduate Research
October 3, 2012

Slides online at kinnejeff.com

About Me

About Me

- Assistant Prof, **Math and Computer Science**

About Me

- Assistant Prof, **Math and Computer Science**
- 3rd year at ISU

About Me

- Assistant Prof, **Math and Computer Science**
- 3rd year at ISU
- **Undergrad projects:**

About Me

- Assistant Prof, **Math and Computer Science**
- 3rd year at ISU
- **Undergrad projects:** SURE 2012,

About Me

- Assistant Prof, **Math and Computer Science**
- 3rd year at ISU
- **Undergrad projects:** SURE 2012, class projects,

About Me

- Assistant Prof, **Math and Computer Science**
- 3rd year at ISU
- **Undergrad projects:** SURE 2012, class projects, independent study

Goals

Goals

- Experience for students, stimulate interest

Goals

- Experience for students, stimulate interest
- Research results

Goals

- Experience for students, stimulate interest
- Research results
- Atmosphere among students, in department

Goals

- Experience for students, stimulate interest
- Research results
- Atmosphere among students, in department

Training researchers: **creativity, working independently, excitement, ...**

Projects

Project – Pseudorandom Number Generators

Project – Pseudorandom Number Generators

- 2, 4, 6, 8, 10, 12

Project – Pseudorandom Number Generators

- 2, 4, 6, 8, 10, 12
- **next = last + 2**

Project – Pseudorandom Number Generators

- 3, 6, 9, 2, 5, 8

Project – Pseudorandom Number Generators

- 3, 6, 9, 2, 5, 8
- **next = (last + 3) % 10**

Project – Pseudorandom Number Generators

- 1, 8, 11, 10, 5, 12

Project – Pseudorandom Number Generators

- 1, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

PRGs

- Linear Congruential Generator

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

PRGs

- Linear Congruential Generator

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

PRGs

- Linear Congruential Generator
- Linear Feedback Shift Register

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

PRGs

- Linear Congruential Generator
- Linear Feedback Shift Register
- Blum Blum Shub

Project – Pseudorandom Number Generators

- **1**, 8, 11, 10, 5, 12
- **next = (5 * last + 3) % 16**

PRGs

- Linear Congruential Generator
- Linear Feedback Shift Register
- Blum Blum Shub
- ...

Why?

Why?

- **Cryptography**

Why?

- **Cryptography**
- **Randomized algorithms**

Why?

- **Cryptography**
- **Randomized algorithms**

PRG Properties

Why?

- **Cryptography**
- **Randomized algorithms**

PRG Properties

- How **secure**

Why?

- **Cryptography**
- **Randomized algorithms**

PRG Properties

- How **secure**
- How **fast** to compute

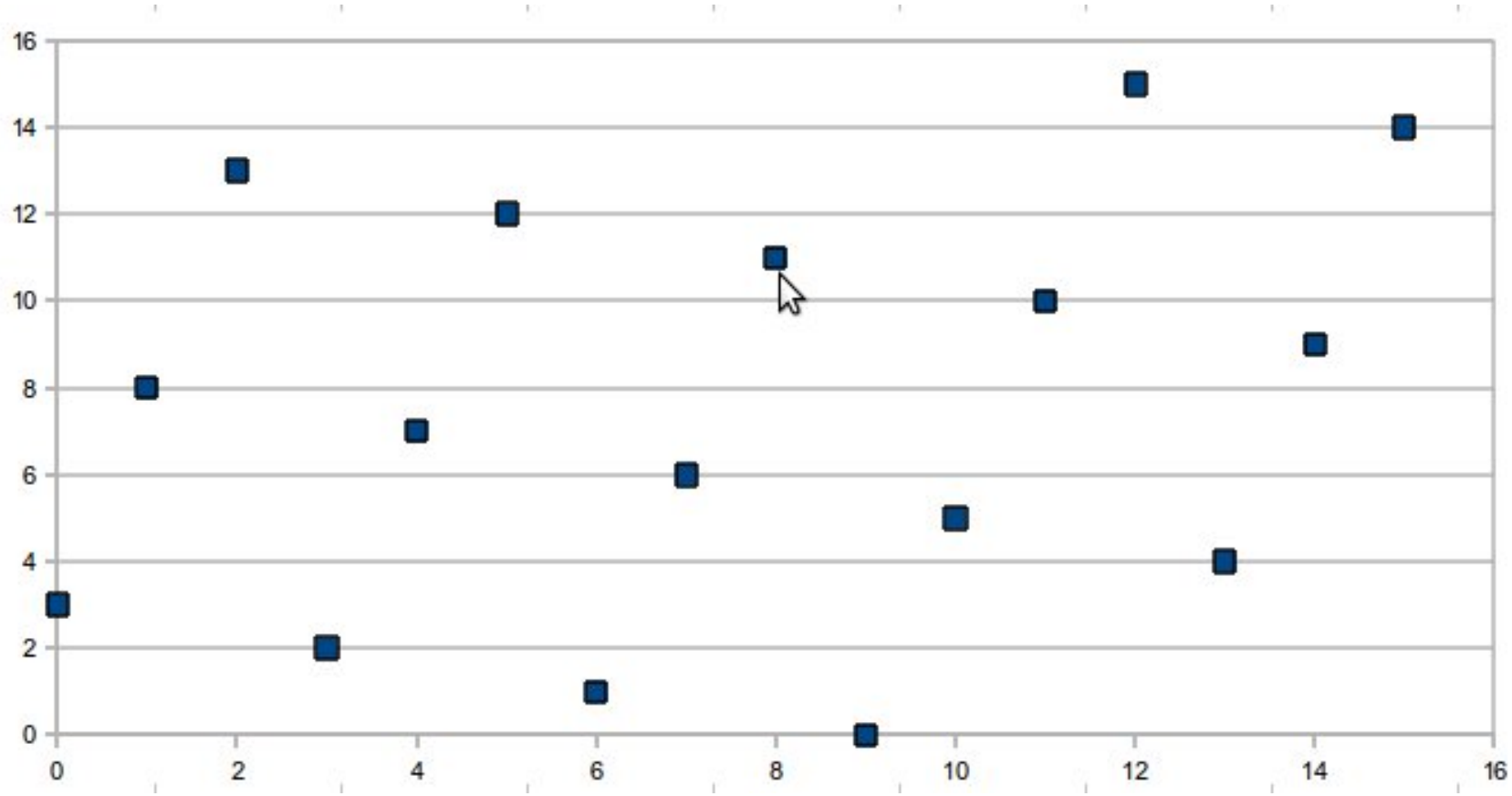
Why?

- **Cryptography**
- **Randomized algorithms**

PRG Properties

- How **secure**
- How **fast** to compute

Our Research...


16
14
12
10
8
6
4
2
0
0
2
4
6
8
10
12
14
16

```
testPrime = int(raw_input("Enter number you wish to check is prime: "))
det = raw_input("y/n Deterministic?: ")
if det == 'y' or det == 'Y' or det == 'yes' or det == 'Yes' or det == 'YES':
    wiki = min(testPrime-1,int(2*(math.log(testPrime)**2)))
    reps = wiki
    det = 1
else:
  reps = int(raw_input("How many times would you like the test run: "))
  det = 0

start = time.time()
answer = MRtest(testPrime,reps,det)
end = time.time()
timer = end-start

if answer == 0: print "Probably prime!, in " + str(timer) + " seconds."
else: print "Composite " + str(answer) + ". It took " + str(timer) + " seconds."
```

Theorem A. *The linear congruential sequence defined by m, a, c, and X_0 has period length m if and only if*

i) *c is relatively prime to m;*

ii) *$b = a - 1$ is a multiple of p, for every prime p dividing m;*

iii) *b is a multiple of 4, if m is a multiple of 4.*

The ideas used in the proof of this theorem go back at least a hundred years. But the first proof of the theorem in this particular form was given by M. Greenberger in the special case $m = 2^e$ [see *JACM* **8** (1961), 383–389], and the sufficiency of conditions (i), (ii), and (iii) in the general case was shown by Hull and Dobell [see *SIAM Review* **4** (1962), 230–254]. To prove the theorem we will first consider some auxiliary number-theoretic results that are of interest in themselves.

Final Results

Final Results

Paper and presentation at a workshop/conference?

Final Results

Paper and presentation at a workshop/conference?

- NCUR,

Final Results

Paper and presentation at a workshop/conference?

- NCUR,
- CSUI

Final Results

Paper and presentation at a workshop/conference?

- NCUR,
- CSUI

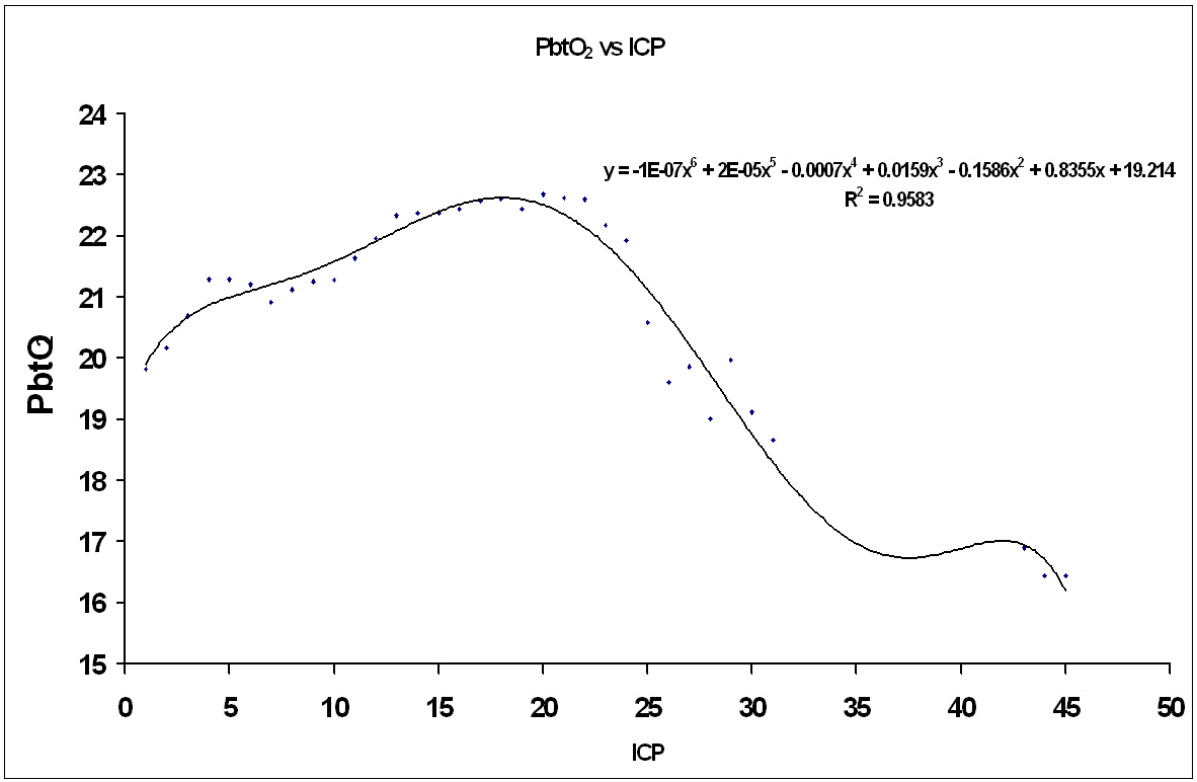
Other Project

Other Project

Brain oxygen monitoring/therapy – genetic algorithms

Other Project

Brain oxygen monitoring/therapy – genetic algorithms



Other Project

Other Project

Neural networks and genetic algorithms

Other Project

Neural networks and genetic algorithms

- Handwriting recognition

Other Project

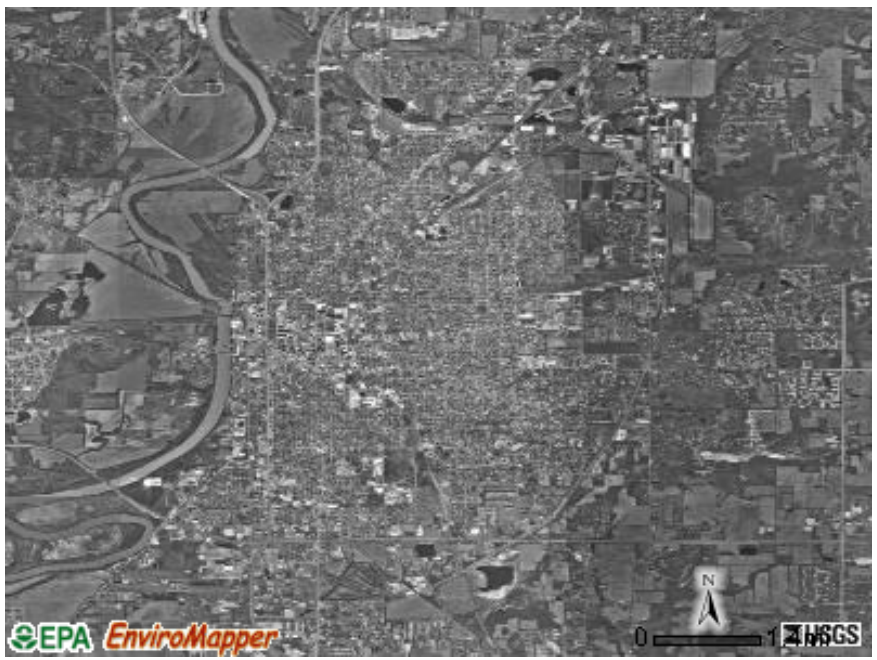
Neural networks and genetic algorithms

- Handwriting recognition
- **Satellite image processing**

Other Project

Neural networks and genetic algorithms

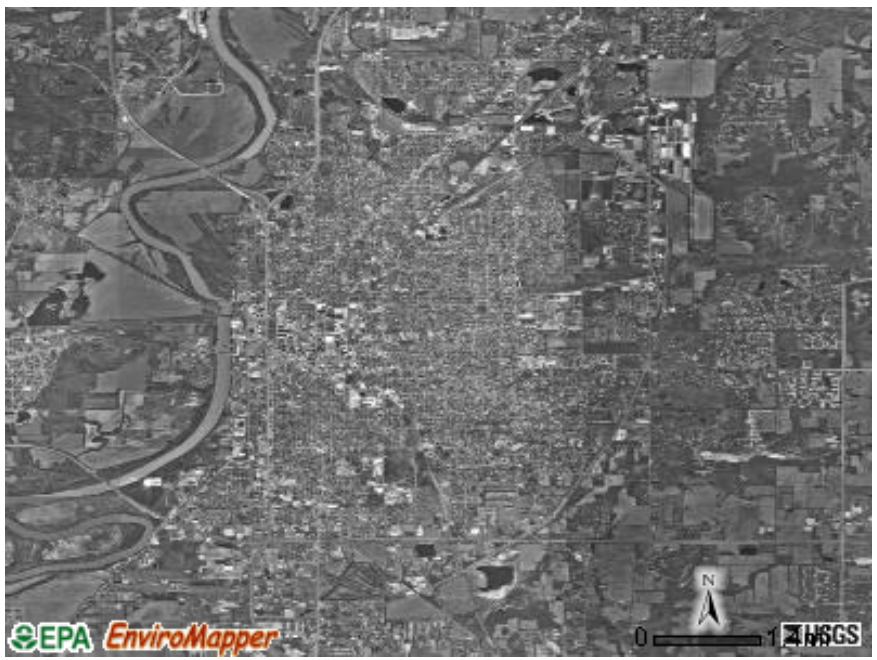
- Handwriting recognition
- **Satellite image processing**



Other Project

Neural networks and genetic algorithms

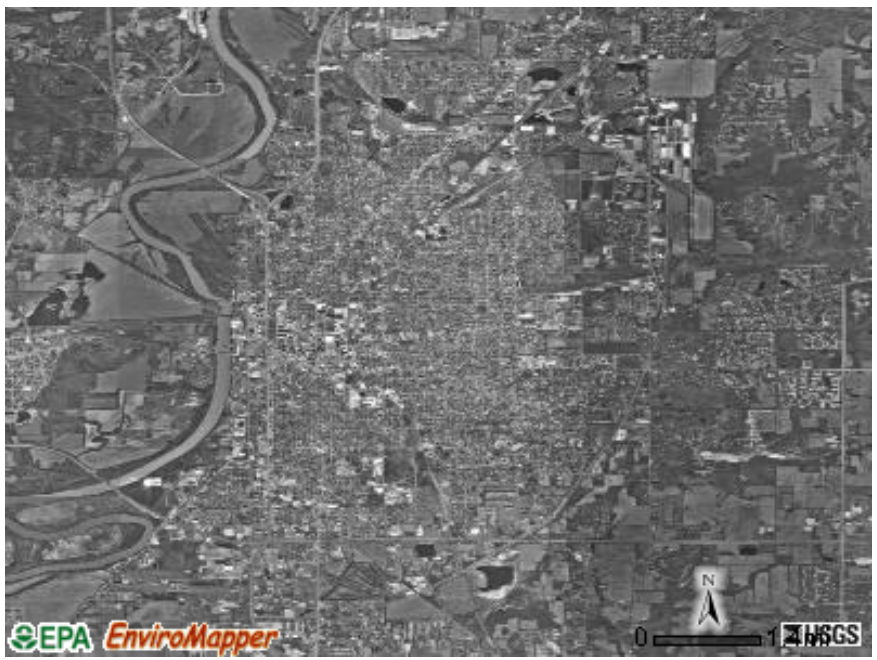
- Handwriting recognition
- **Satellite image processing**
- Game playing



Other Project

Neural networks and genetic algorithms

- Handwriting recognition
- **Satellite image processing**
- Game playing



Reflection

Funding

Funding

- **Successful:**

Funding

- **Successful:** University Research Committee,

Funding

- **Successful:** University Research Committee, CSRC,

Funding

- **Successful:** University Research Committee, CSRC, Student wages

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:**

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science,

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF,

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF, ...

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF, ...

Unfunded Student Research

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF, ...

Unfunded Student Research

- Class project

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF, ...

Unfunded Student Research

- Class project
- Independent study (for credit)

Funding

- **Successful:** University Research Committee, CSRC, Student wages
- **Maybe:** Indiana Academy of Science, NSF, ...

Unfunded Student Research

- Class project
- Independent study (for credit)

Lessens Learned

Lessens Learned

Many students need...

Lessens Learned

Many students need...

- Specific **work hours, days**

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained**

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained** (e.g., write up results in paper, present at workshop/conference)

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained** (e.g., write up results in paper, present at workshop/conference)

Big Question

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained** (e.g., write up results in paper, present at workshop/conference)

Big Question

Have them work on **my projects or choose their own**?

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained** (e.g., write up results in paper, present at workshop/conference)

Big Question

Have them work on **my projects or choose their own**?

- **Former:** my expertise, better chance at results

Lessens Learned

Many students need...

- Specific **work hours, days**
- **Research process explained** (e.g., write up results in paper, present at workshop/conference)

Big Question

Have them work on **my projects or choose their own**?

- **Former:** my expertise, better chance at results
- **Latter:** their interest/independence/motivation

Discussion

Ask yourself...

- Why supervise undergraduate research?

Ask yourself...

- Why supervise undergraduate research?
- What project ideas?

Ask yourself...

- Why supervise undergraduate research?
- What project ideas?
- What is a successful outcome?

Ask yourself...

- Why supervise undergraduate research?
- What project ideas?
- What is a successful outcome?
- Interdisciplinary research?

The end.

Slides online at http://www.kinnejeff.com