

About Research

Gwoboa Horng

AI Lab

CS, NCHU

Why research?

- Main difference between graduate and undergraduate study:

RESEARCH

What is RESEARCH?

Careful, systematic, patient
study and investigation
in some field of knowledge,
undertaken to **discover** or **establish**
facts or **principles**

(Source: Webster's New World Dictionary)

What is RESEARCH?

"Research is what I'm doing when I don't know what I'm doing."

Wernher von Braun

(generally regarded as the father of the United States space program)

What is RESEARCH?

Research is to Re-Search.

(溫故知新)

RESEARCH includes

- **Find suitable topics/problems**
- Decide plausible methods
- Obtain concrete results
- Write technical papers
- Publish papers
- Give oral presentations

Find a suitable topic/problem(1/4)

- 提出一個問題往往比解決一個問題更重要

因為

解決一個問題也許僅僅是一個數學上或實驗上的技巧而已
而提出新的問題 新的可能性 從新的角度去看舊的問題
卻需要有創造性的想像力 而且標誌著科學的真正進步

– 愛因斯坦

- *In mathematics the art of proposing a question must be held of higher value than solving it.*

—Georg Cantor

From questions to problems

- Asking questions is the very heart of the scientific enterprise.
- Quite literally, everything in science begins with the questions.
- Not just any questions, however. In general, questions begin with words like "what", "when", "where", "how", "how big", "how many", and most importantly, "why".

Find a suitable topic/problem(2/4)

- Public key cryptography (history)
 - Merkle had registered in the Fall of 1974 for a course in computer security at U.C. Berkeley. Each student is required to submit a project proposal early in the term.
 - Merkle addressed the problem of public-key distribution or as he called it “**Secure Communication over Insecure Channels**”.
 - The instructor could not understand Merkle’s proposal. He demanded that it be rewritten. After one more iteration of this process, Merkle dropped the course.

Find a suitable topic/problem(3/4)

- Well-known problem
 - Fermat last theorem, $P=NP$?
- Original problem
 - Motivations
- **From reading papers**
- Assigned
 - Research projects

Find a suitable topic/problem(4/4)

Topics obtained from reading papers

- Improvement/enhancement
- Generalization
- Specialization
- Combination

Topics obtained from reading papers 1/4

- **Improvement/enhancement**

time/computational cost

space

bandwidth/message size

security/trust

power consumption

random bits

Topics obtained from reading papers 2/4

- **Generalization**

 - Secret Sharing

 - access structure

 - Protocols

 - two-party, multiparty

 - Change constants into Variables

Secret Sharing

- A *secret sharing scheme* is a system that is designed to protect a secret piece of information among a group of users in such a way that only certain subsets of users can jointly reconstruct the secret, whereas other subsets of users can ideally not obtain any information about the secret.
- The collection of subsets that can access the secret is called the *access structure* of the secret sharing scheme.

Secret Sharing

- K-out-of-n ((k,n)- *threshold schemes*)
- General *access structure*
- *Non-Monotonic Access Structures*

secret sharing *with added extras*

1. the ability to disenroll a dishonest user.
2. the ability to change the access structure dynamically
3. protecting against insider cheating.
4. establishing a secret sharing scheme in the absence of a trusted third party.
5. sharing more than one secret.
6. sharing one secret more than once.
7. reconstructing the secret without knowledge of user identities (*anonymous* secret sharing).

Topics obtained from reading papers 3/4

- **Specialization**

Hard problems

Discrete logarithm

Baby-Step Giant-Step method

Pohlig-Hellman method

Change variables into constants

Topics obtained from reading papers 4/4

- **Combination**

e.g. *A blind*

RSA-based

group

signature scheme

(<http://www.cse.ucsd.edu/users/mihir/crypto-topic-generator.html>)

How to read papers?

- Efficient reading of papers in science and technology

- Reference:

“Teaching Students to Read Papers”

D. S. Franzblau

Reading Research Papers

Some tricks 1/2

- Give up the notion that you must verify the truth of every single line or that you must understand each paragraph before going on to the next.
- Decide what parts of the paper to read carefully and what to skip.
- Get down to details.
- Work through a small section at a time (don't try to understand everything at once).
- Avoid the temptation to go through a section line by line.

Reading Research Papers

Some tricks 2/2

- Make it your own by thinking about how you might approach the problem.
- Don't look things up until you are sure you have to.
- Try to read around those words you don't know.
- Put aside the part you get stuck and try a different part of the paper.
- Ask for help when necessary.

Reading Research Papers

Type of information to look for 1/3

- What is the paper about?

What problem does the author address?

Why is the problem interesting?

What is the history of the problem?

What are the results?

Is the problem solved or only partial results given?

What are the key steps leading to the results?

Reading Research Papers

Type of information to look for 2/3

- **What is new, interesting or important here?**

What makes the paper worth reading?

the problem itself

the final results or solution

the method used

some other feature

What are the authors' contributions?

Reading Research Papers

Type of information to look for 3/3

- Which parts are worth spending time on?

Research methods

- Abstraction of the problems (and methods)
- Models
- Assumptions
- Tools from other fields

Research methods

Abstraction of the problem

- The seven bridges of Königsberg

Multigraph model (Euler 1736)

Euler circuit/path

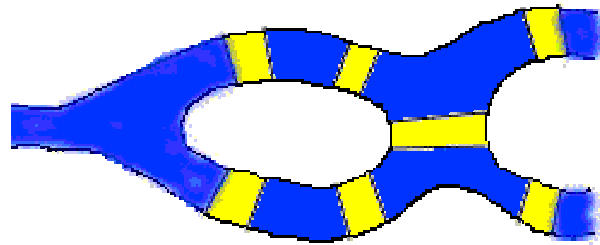
Necessary and sufficient conditions for

Euler circuits and paths

Graph theory

The seven bridges of Königsberg

- In Königsberg, Germany, a river ran through the city such that in its center was an island, and after passing the island, the river broke into two parts. Seven bridges were built so that the people of the city could get from one part to another. A crude map of the center of Königsberg might look like this:



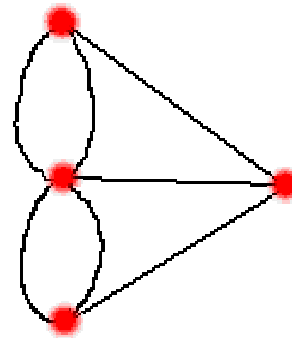
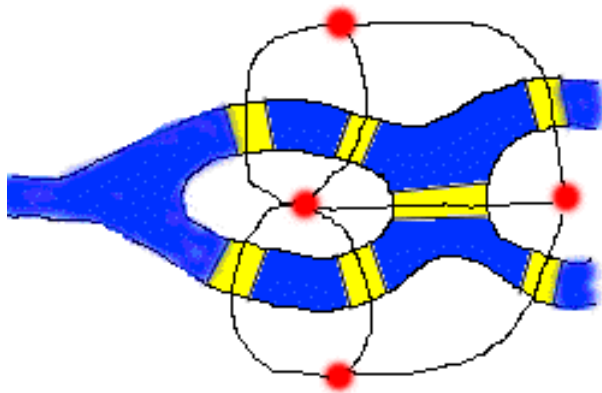
The seven bridges of Königsberg

- The people wondered whether or not one could walk around the city in a way that would involve crossing each bridge exactly once.

The seven bridges of Königsberg

Euler's Solution

- Euler realized that all problems of this form could be represented by replacing areas of land by points (he called them *vertices*), and the bridges to and from them by arcs. For Königsberg, let us represent land with red dots and bridges with black curves:



The seven bridges of Königsberg

Euler's Solution

- The problem now becomes one of drawing this picture without retracing any line and without picking your pencil up off the paper. (The **general abstract problem** of the seven bridges of Königsberg.)

The Generalization to Graph Theory

- Euler generalized this mode of thinking by making the following definitions and proving a theorem:

Definition: A network is a figure made up of points (vertices) connected by non-intersecting curves (arcs).

Definition: A vertex is called odd if it has an odd number of arcs leading to it, other wise it is called even.

Definition: An Euler path is a continuous path that passes through every arc once and only once.

Theorem: If a network has more than two odd vertices, it does not have an Euler path.

The Generalization to Graph Theory

- Euler also proved the converse:

***Theorem:* If a network has two or less odd vertices, it has at least one Euler path.**

Research methods

- Models
 - RAM (analysis of algorithms)
 - Network security model
- Techniques
 - Majority vote
 - Amortized analysis

Research methods

- Assumptions
- Knowledge from other fields

NN, GA

Research methods

- Assumptions

Research methods

- Knowledge from other fields
NN, GA
- **Fruit Flies Could Hold Key to Future Internet**
 - http://www.internetevolution.com/author.asp?doc_id=205027&f_src=itgazette
 - MIT and most universities now have departments dedicated to what is called [amorphous computing and/or swarm intelligence](#).
(非晶計算)
- **Amorphous computing** refers to computational systems that use very large numbers of identical, parallel processors each having limited computational ability and local interactions.

<http://en.wikipedia.org/wiki/Amorph>

Results and contributions

- **Analysis and formal proof**
complexity, correctness, security
algebra, algorithm, complexity theory,
number theory, probability, ...(**Math**)
- **Simulation**
- **Comparisons**
implemented correctly?

Results and contributions

- Right/wrong: objective (fact, provably true)
- Good/bad: subjective (opinion, interpretation)

Writing technical papers

- **Helpful Hints for Technical Paper Writing**

http://swig.stanford.edu/~fox/paper_writing.html#hints

Submit papers for publication

- **Conferences/workshops**
- **Journals**
- **Handling rejections**

Presentations

- **Oral Presentation Advice**

<http://www.cs.wisc.edu/~markhill/conference-talk.html>

The end

- Questions?