Cybersecurity At CI

April 20, 2018

Michael Soltys
http://www.msoltys.com
michael.soltys@csuci.edu
@MichaelMSoltys

NATIONAL
CYBERWATCH
CENTER

cyberwatch west

The Center for Cybersecurity Education

NSF

http://nasaswarmathon.com

ACM Regional Competitions 2018

ACM Regional Competitions 2018

The 2018 World Finals

ACM Regional Competitions 2018

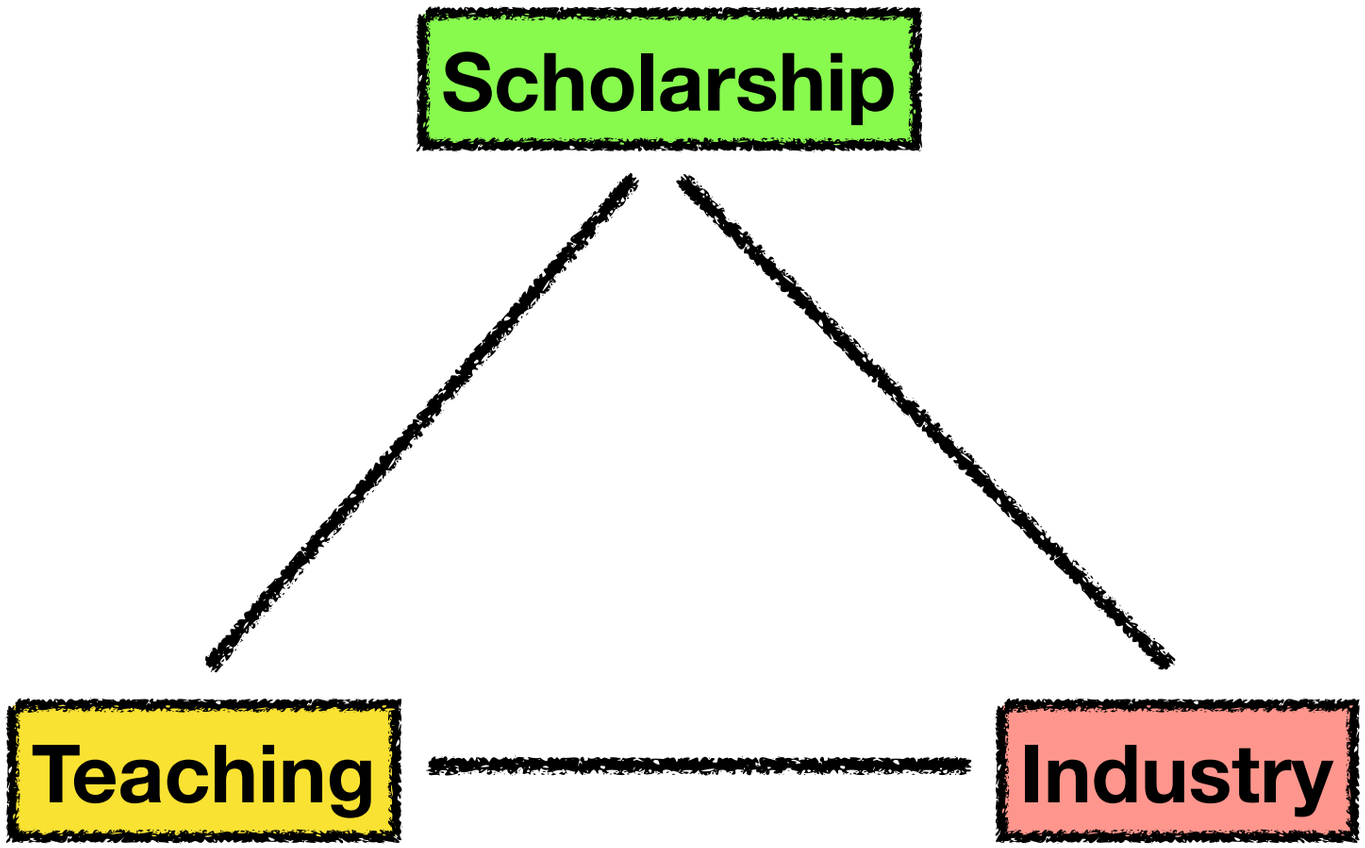
The 2018 World Finals

1. Moscow State University
2. Moscow Institute of Physics and Technology
3. Peking University
4. The University of Tokyo
5. Seoul National University
6. University of New South Wales
7. Tsinghua University
8. Shanghai Jiao Tong University
9. St. Petersburg ITMO University
10. University of Central Florida

https://icpc.baylor.edu/regionals/finder/world-finals-2018

Sobering Stats

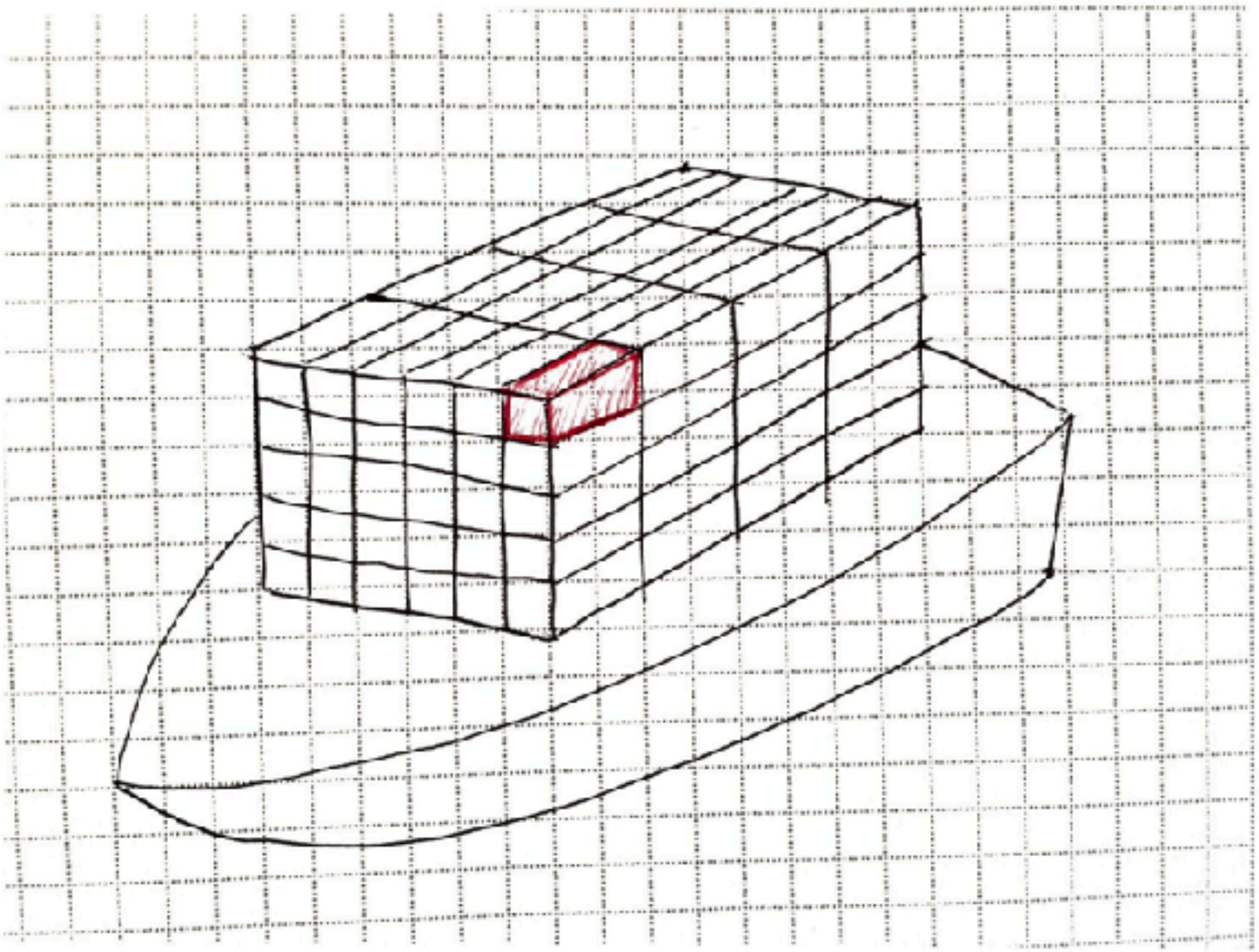
- NSB: engineering degrees dropped 20% since 1985
- ACT: less than 6% high school seniors plan to take engineering
- AFS: 0.8% students plan to major in math
- Intel Science Fair: 6million Chinese students applied; 65K US students did (~100:1)
- 50% of US Engineering PhDs go to foreign students
- In next decade, 90% of world scientists & engineers will reside in Asia

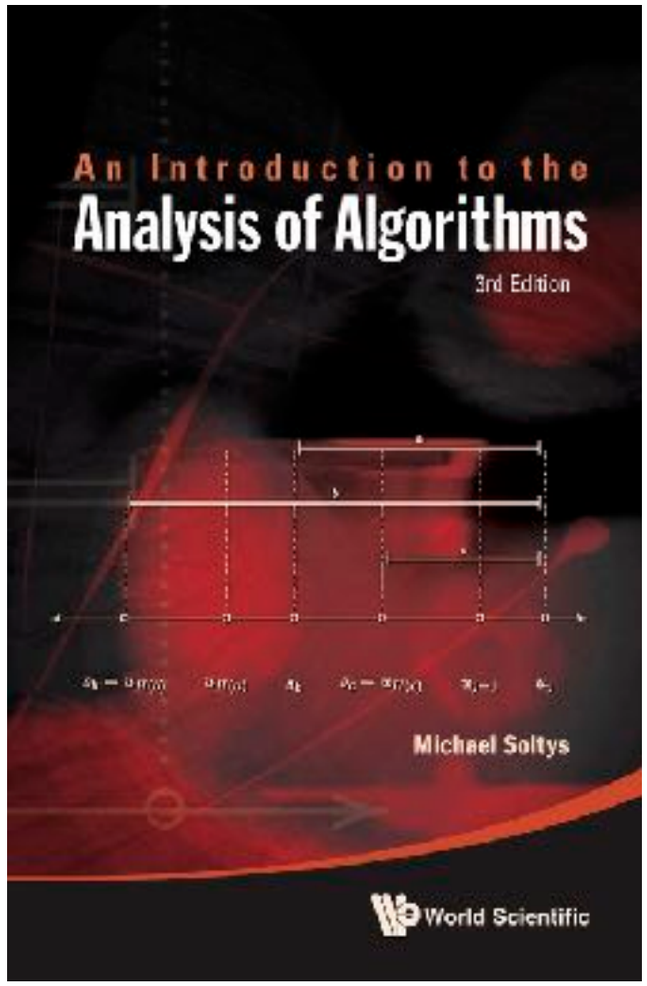

Scholarship
Teaching
Industry

We are going to use the following arrays:

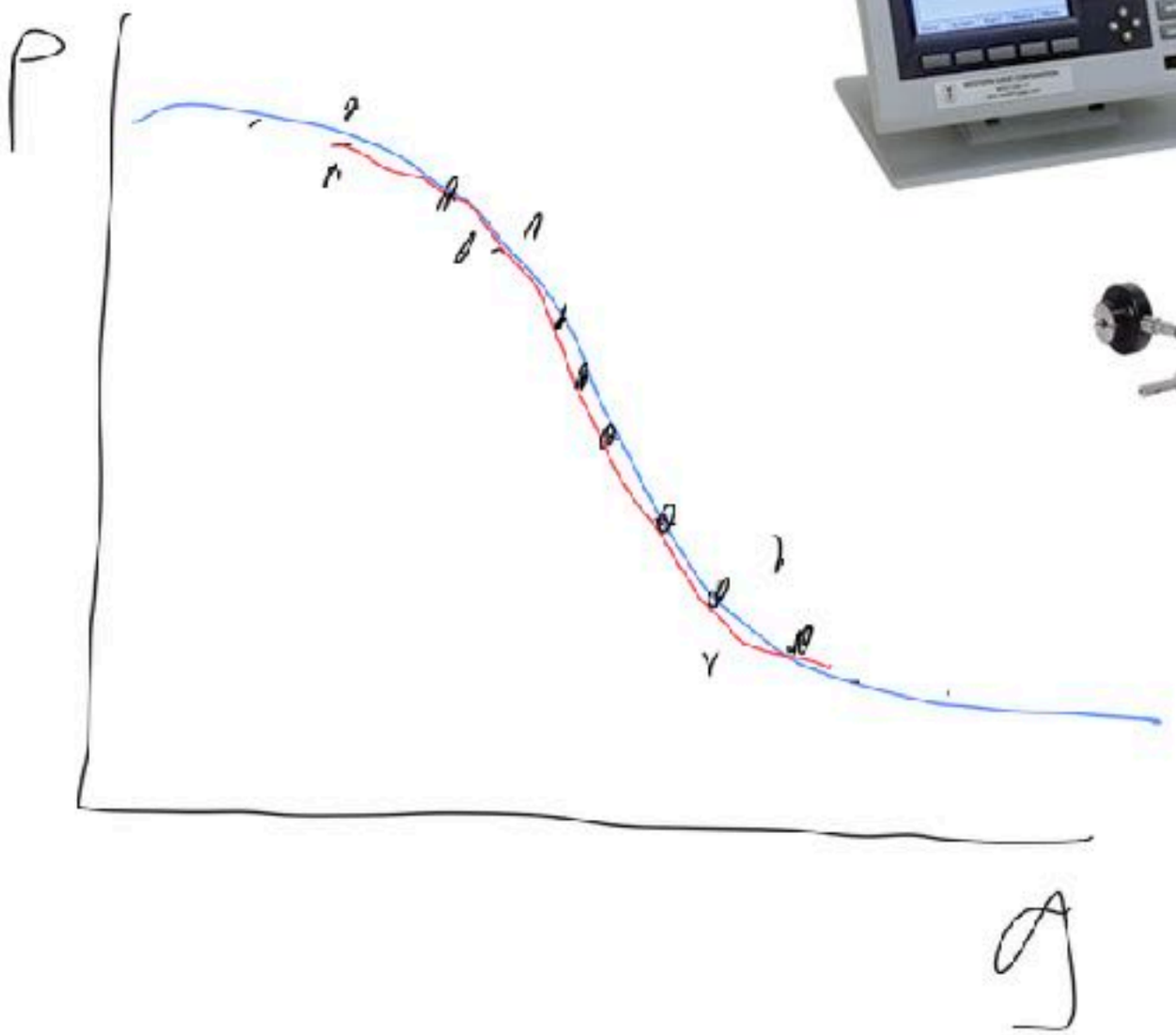
```
Ship[i,j,k]
Stacks[i,j,k]
Chassis[i,j]
Auxiliary[i,j,k]
```

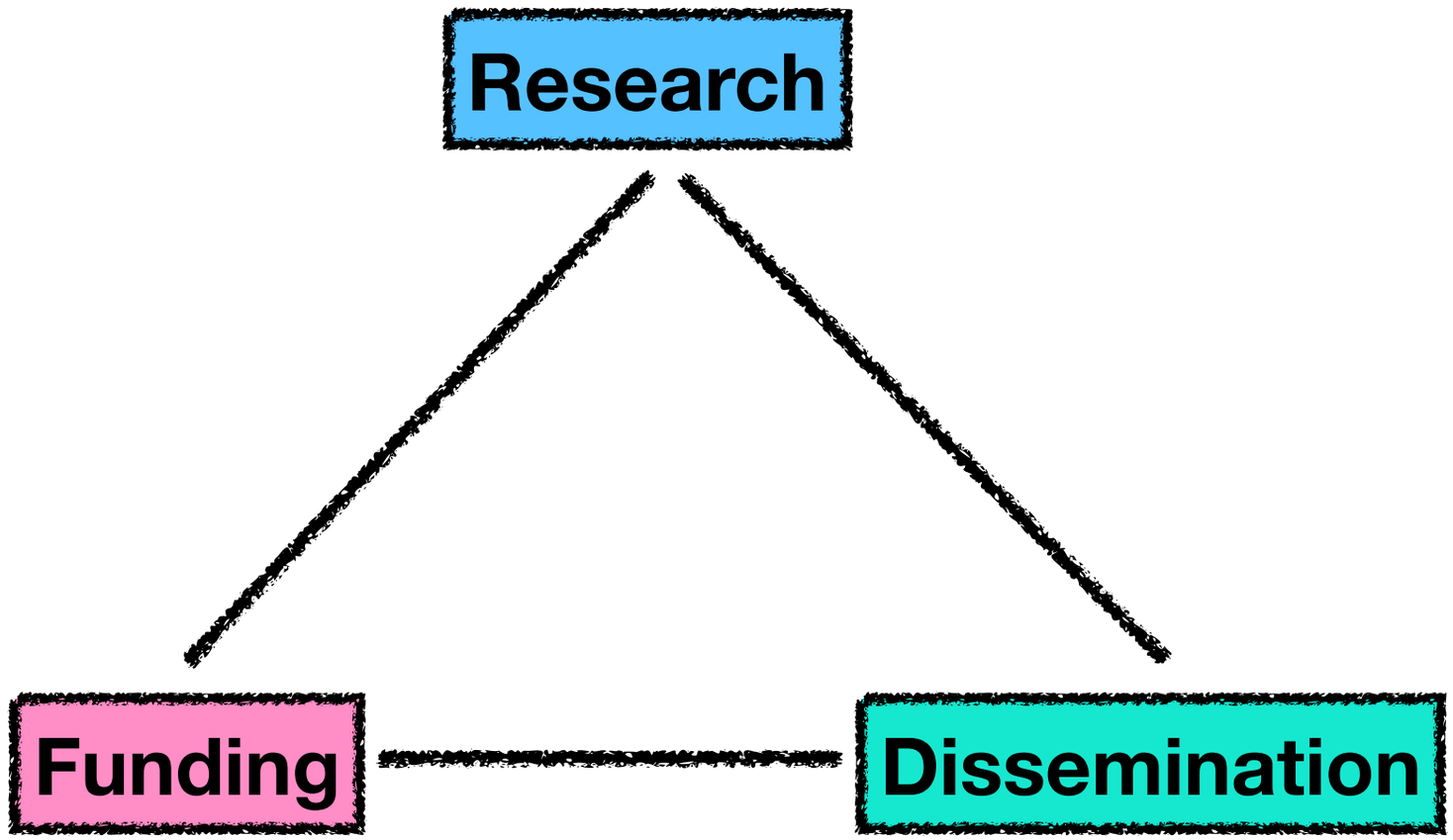
These array will contain identifiers (given as positive integers) of all the containers. So for example, `Ship[2,3,5] = 97` means that in the second row, third column, at depth 5, we have contained number 97. As in the picture below, the red container is in position `[1,1,1]`.





Graph fitting
Pressure vs Gap




Research
Funding
Dissemination

Introducing 4 projects

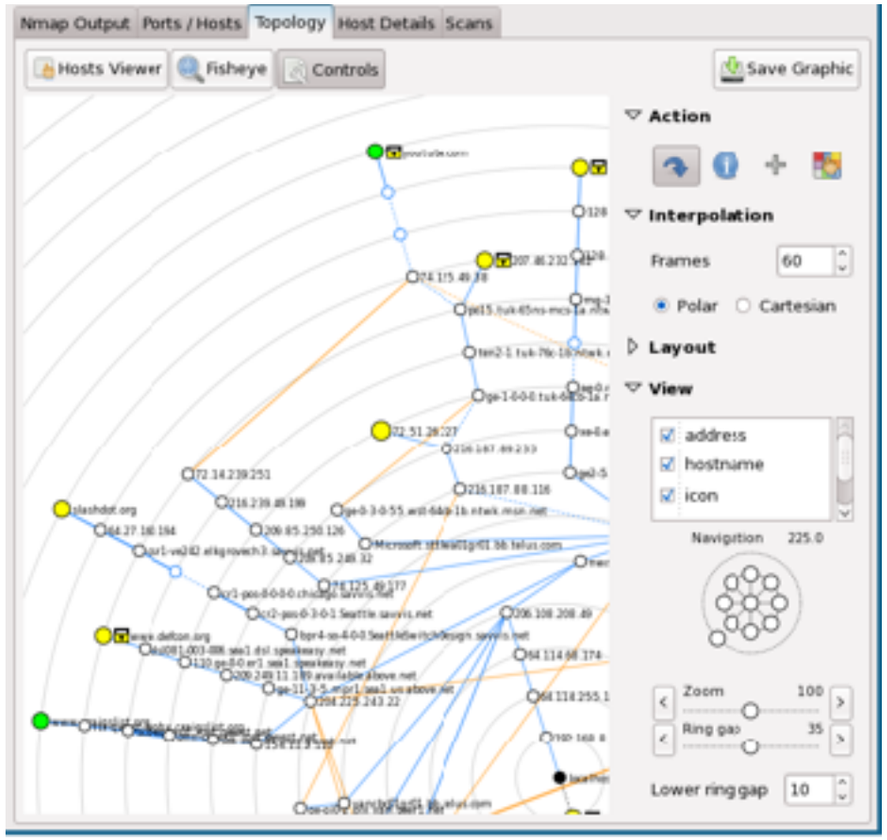
- **Cybersecurity at HAAS**
- Zane Gittins
- Hank Lacayo Institute

Cybersecurity Haas Automation

By Zane Gittins
Under the guidance of Dr. Soltys
Made possible by the Hank Lacayo Program

My Role: Proactive In-House Cybersecurity

- Frequently take on the role of an outside attacker.
- Stay up to date on the latest cyber threats.
- Coordinating with network engineers and IT.

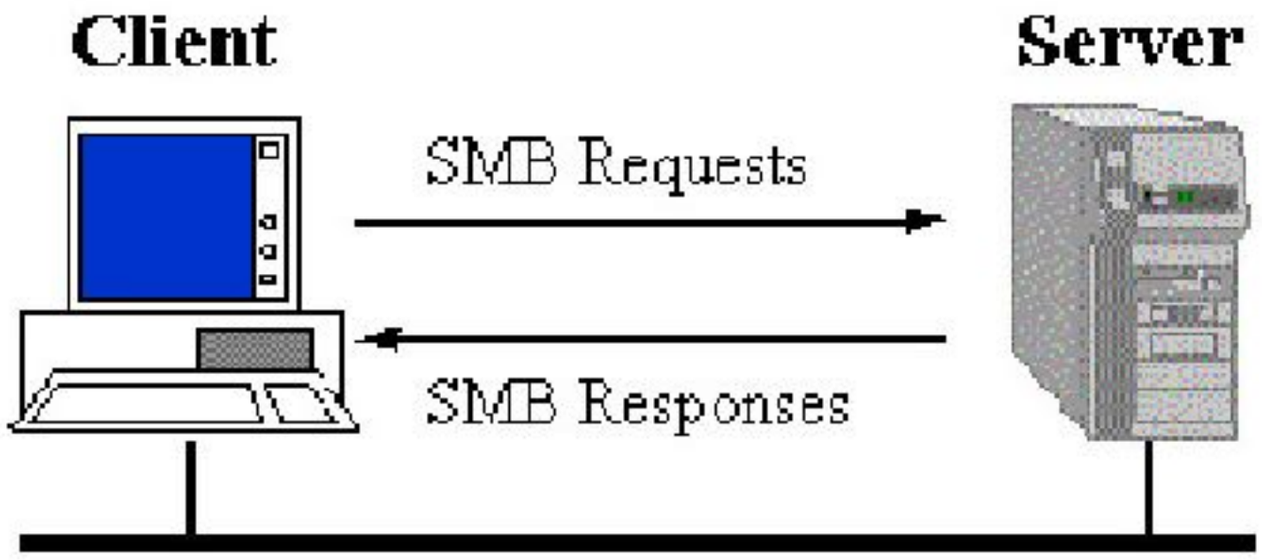


Eternal Blue: Background

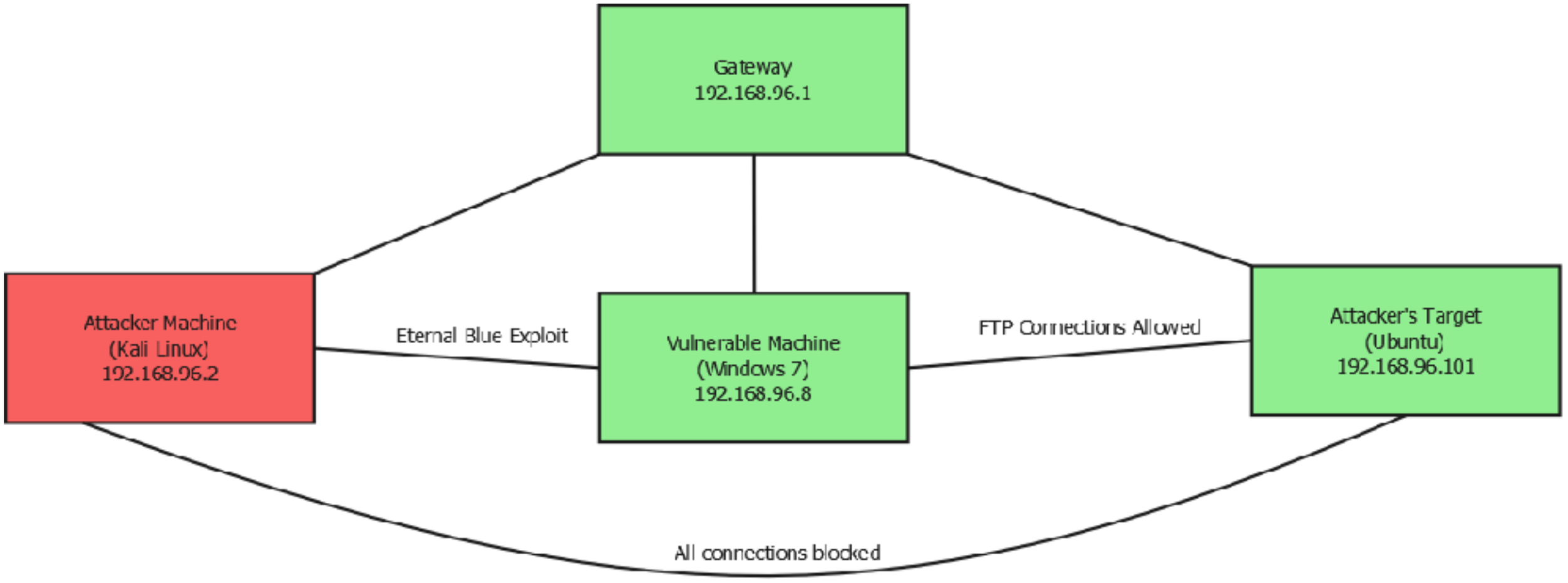
- Leaked by group called the Shadow Brokers.
- Developed by the National Security Agency.

Eternal Blue: SMB Vulnerability

- Makes use of vulnerabilities in service message block protocol v1.



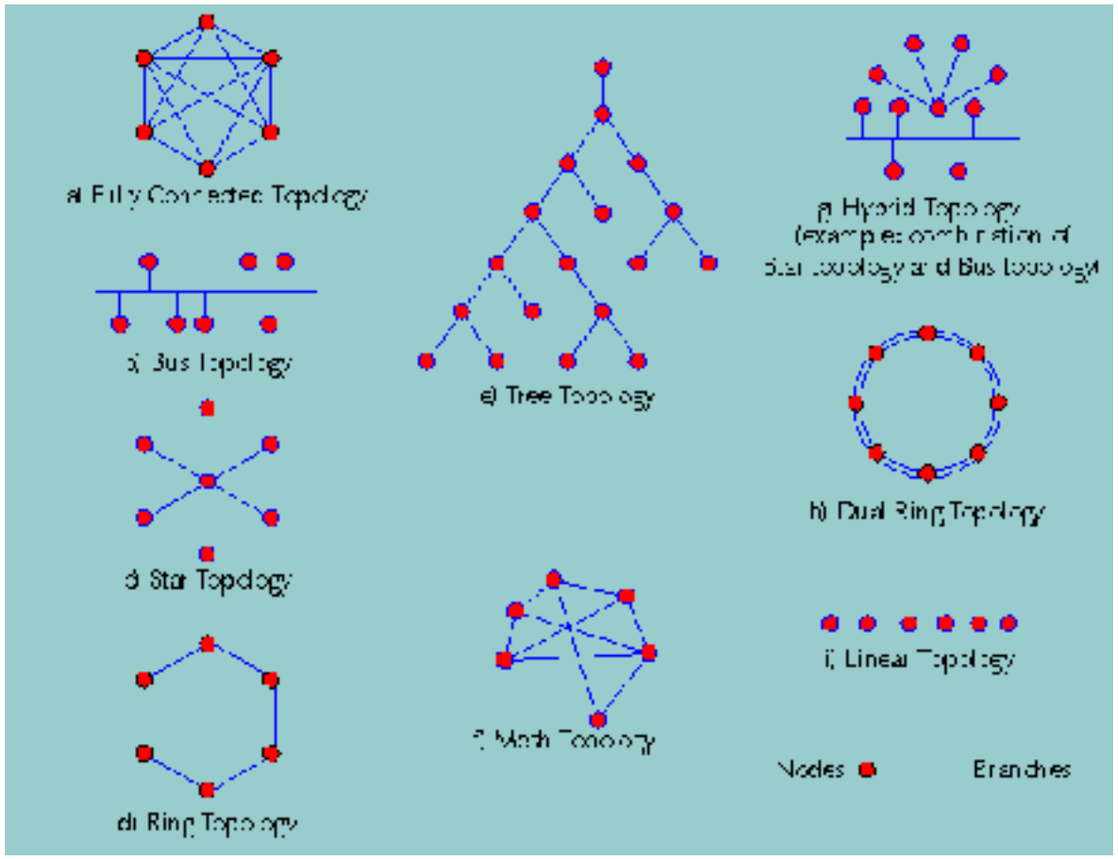
Eternal Blue: Demonstration



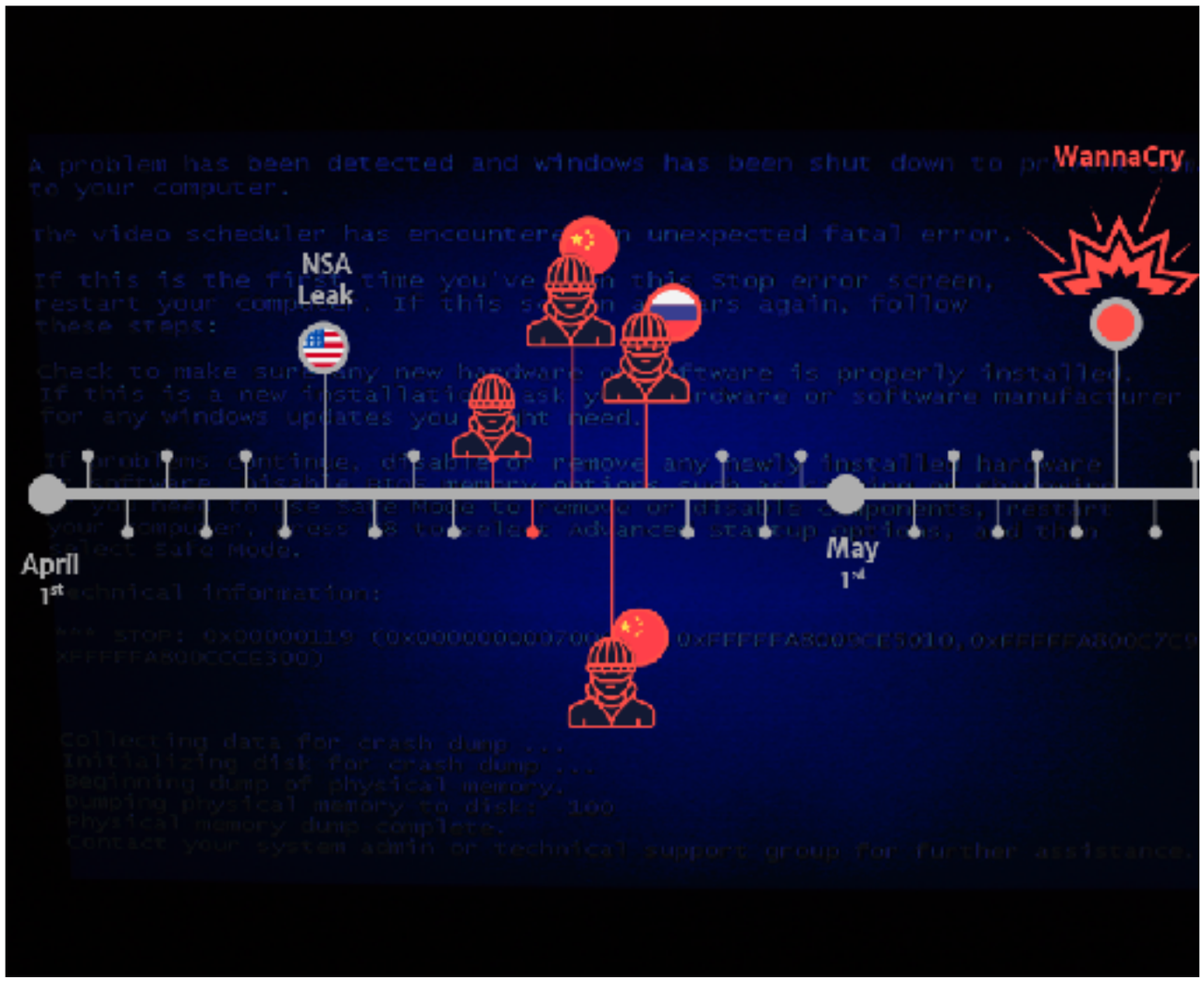
Eternal Blue: Demonstration

Demonstration

Network Topology



Wannacry Malware



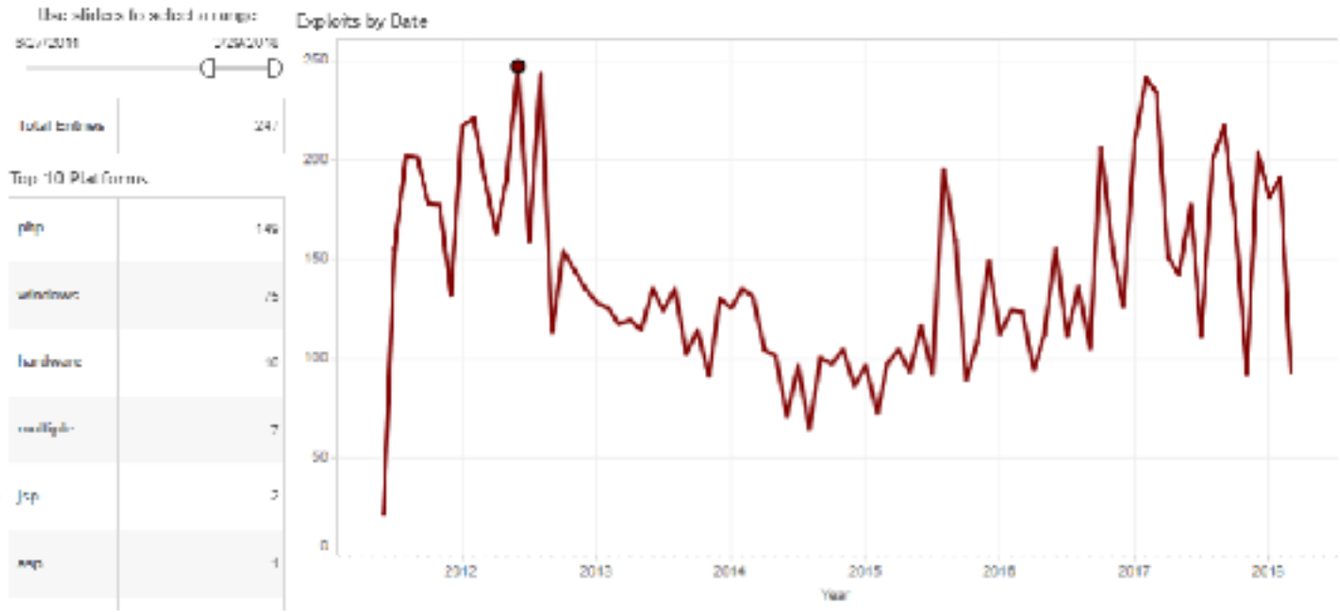
- Mitigate vulnerabilities as soon as possible.
- Estimated hundreds of millions to billions of dollars in damages.

Wannacry Malware

- Ransomware made possible by cryptocurrencies.

Advantages of In-House Penetration Testing

- Length of engagement.
- Deeper understanding of assets, policies, and infrastructure.
- Rapid testing of novel vulnerabilities.
- State backed exploit development and cyber campaigns.
    - Eternal Blue, Eternal Romance, Stuxnet.



- **SEAKER**

- **Eric Gentry**, Geet, Ryan McIntyre

- Working with HTTF

Portable
Digital Forensics Triage Tool
Storage Evaluator And Knowledge Extraction Reader

Eric Gentry
California State University Channel Islands

Modern Forensic Lab

- Cumbersome
- Expensive
- Stationary
- Labor Intensive
- Analysis in **days**

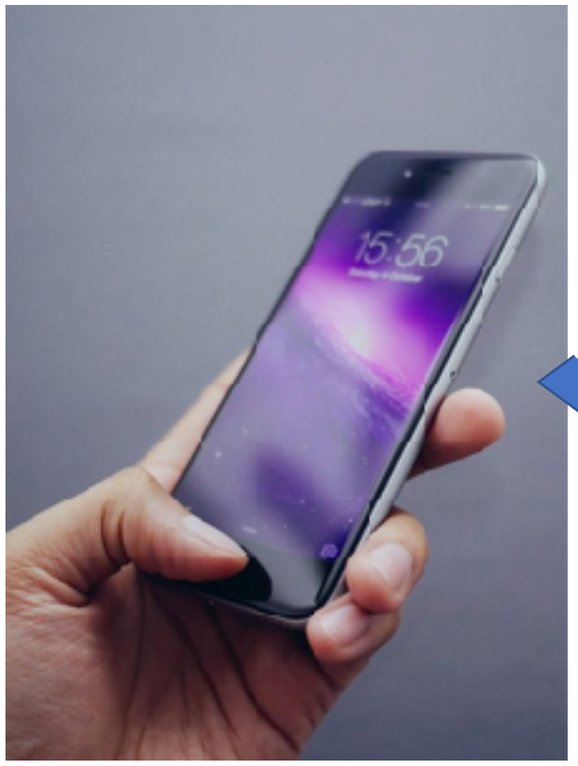
- Not suitable for the field

http://dujs.dartmouth.edu/2013/03/computer-forensics-in-criminal-investigations/#.Wr7qlJPwb6w

Modern Mobile Forensic Lab

- Simple
- Inexpensive
- Mobile
- Easy to use
- Analysis in **minutes**

- Field-Ready



http://nocamels.com/2018/02/cellebrite-hack-phone
http://tech-lives.com/data-recover-from-memory-card-hard-drive/

Technology Behind SEAKER

nvestigators

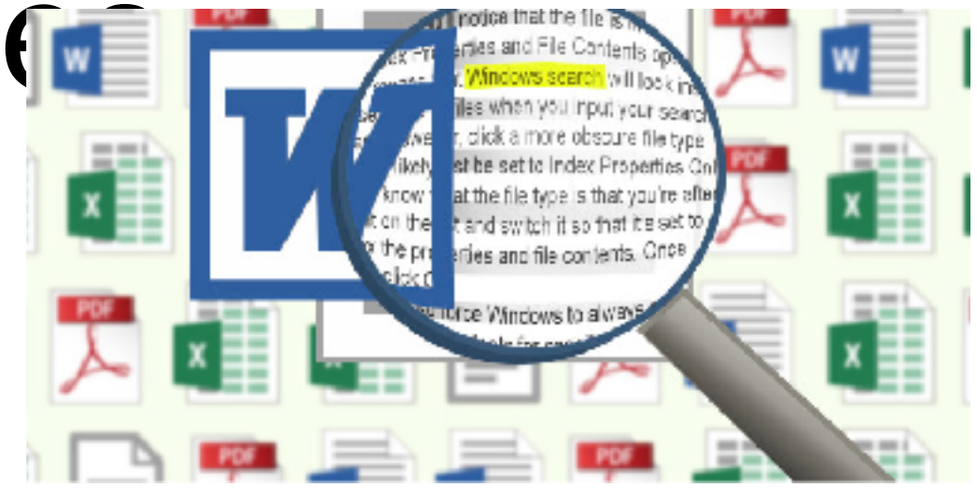
raspberry pi
+
analysis code

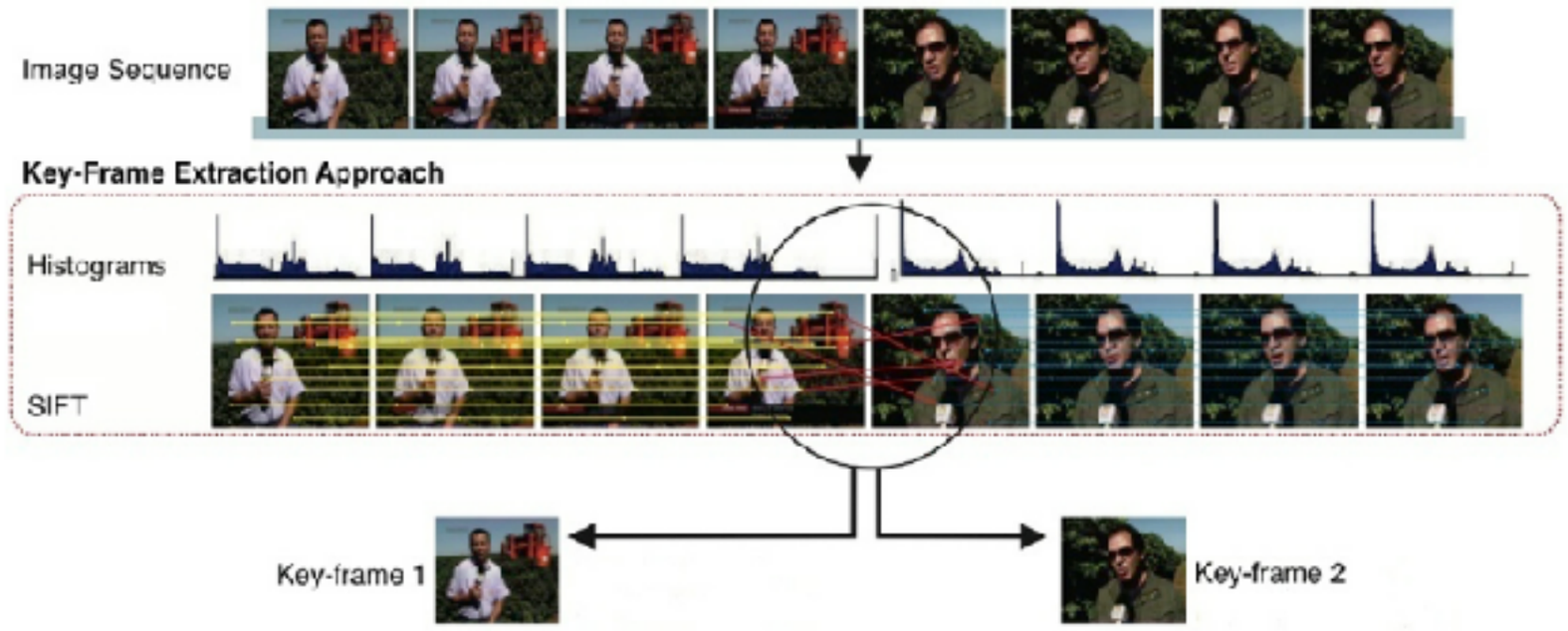
Digital Evidence

http://www.softicons.com/system-icons/simple-icons-by-harwen-zhang/hard-drive-icon

Analysis Techniques

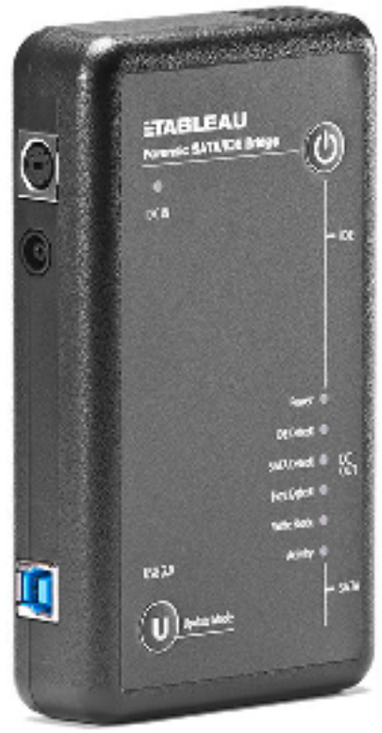
- File content
- Browser history
- Deleted files
- Images
- Videos





https://www.makeuseof.com/tag/search-file-contents-windows/

Forensic Use Verification



- Write Block Independent Verification
  - Tableau Forensic SATA/IDE Bridge Kit (T
- NIST
  - Computer Forensics Tool Testing Prograr
    - Hardware Write Block
    - Mobile Devices

National Institute of Standards and Technology
U.S. Department of Commerce

https://www.nist.gov

https://www.guidancesoftware.com/tableau/hardware/t35u

Universal Usage Potentia

- Ventura County District Attorney
- SCHTTF (Southern California High Tec Force)
- Corporate IT
- Military applications

http://www.microone.com/Corporate.htm
https://www.defenseindustrydaily.com/rugged-notebooks-american-military-06767/

- **Image Recognition**
- Geet
- Difference Hashing
- HTTF

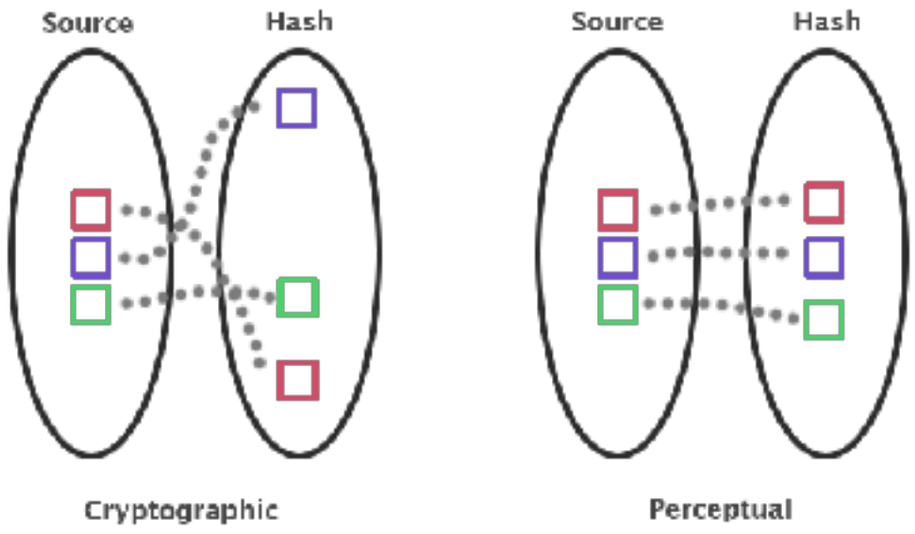


Image Recognition

-Geetanjali Agarwal

Under the guidance of Dr. Michael Soltys


technology
internet
data
digital
computer
media
graphic
art
image processing

Image Recognition

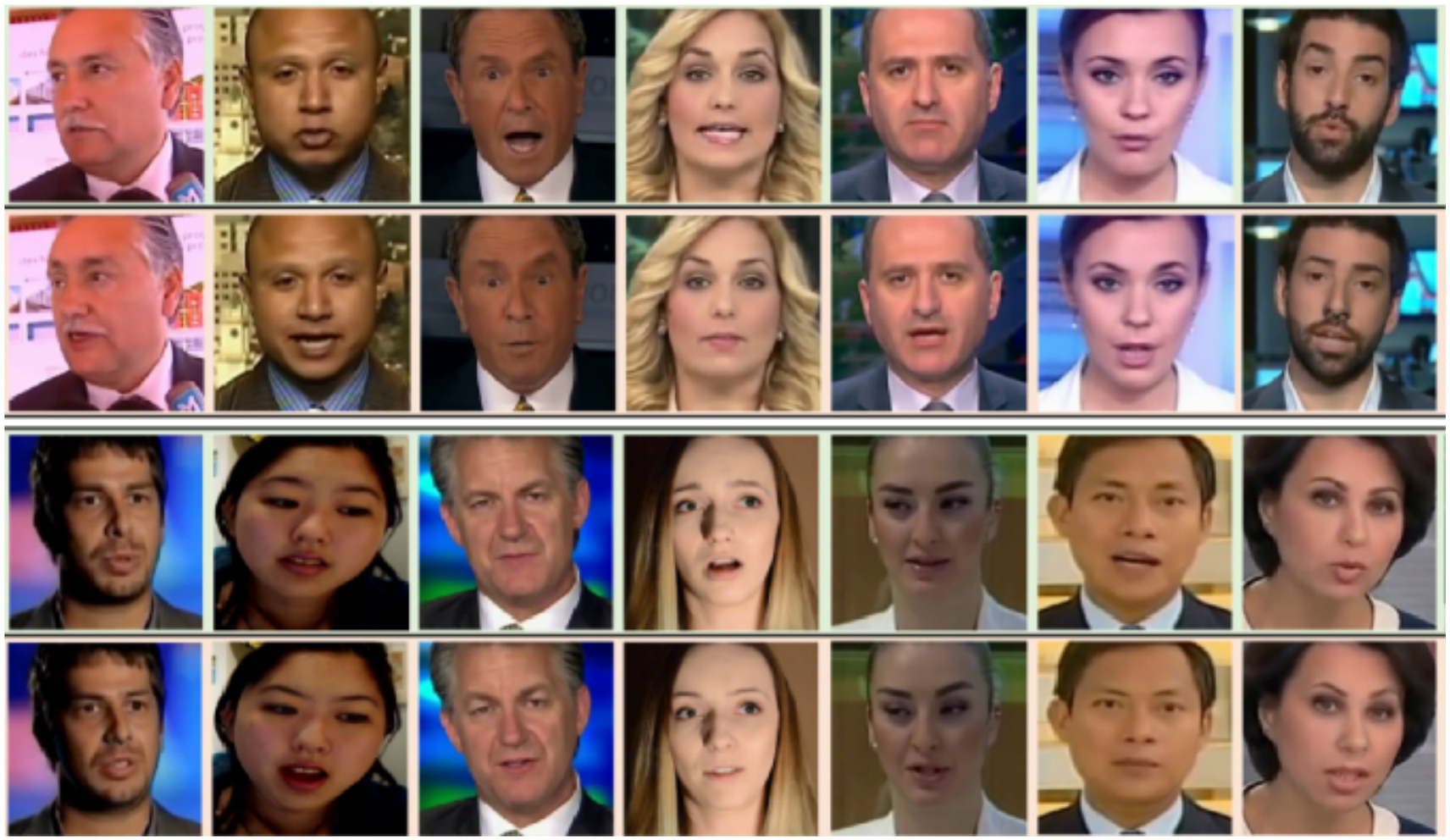


Image Fingerprinting/Hashing

Difference Hash Algorithm

- dhash is based on image gradient
- Steps involved –

Input Image

Reduce size (but then magnified for viewing)

Reduce color (Grayscale the image)

14a602b12610 2ft678

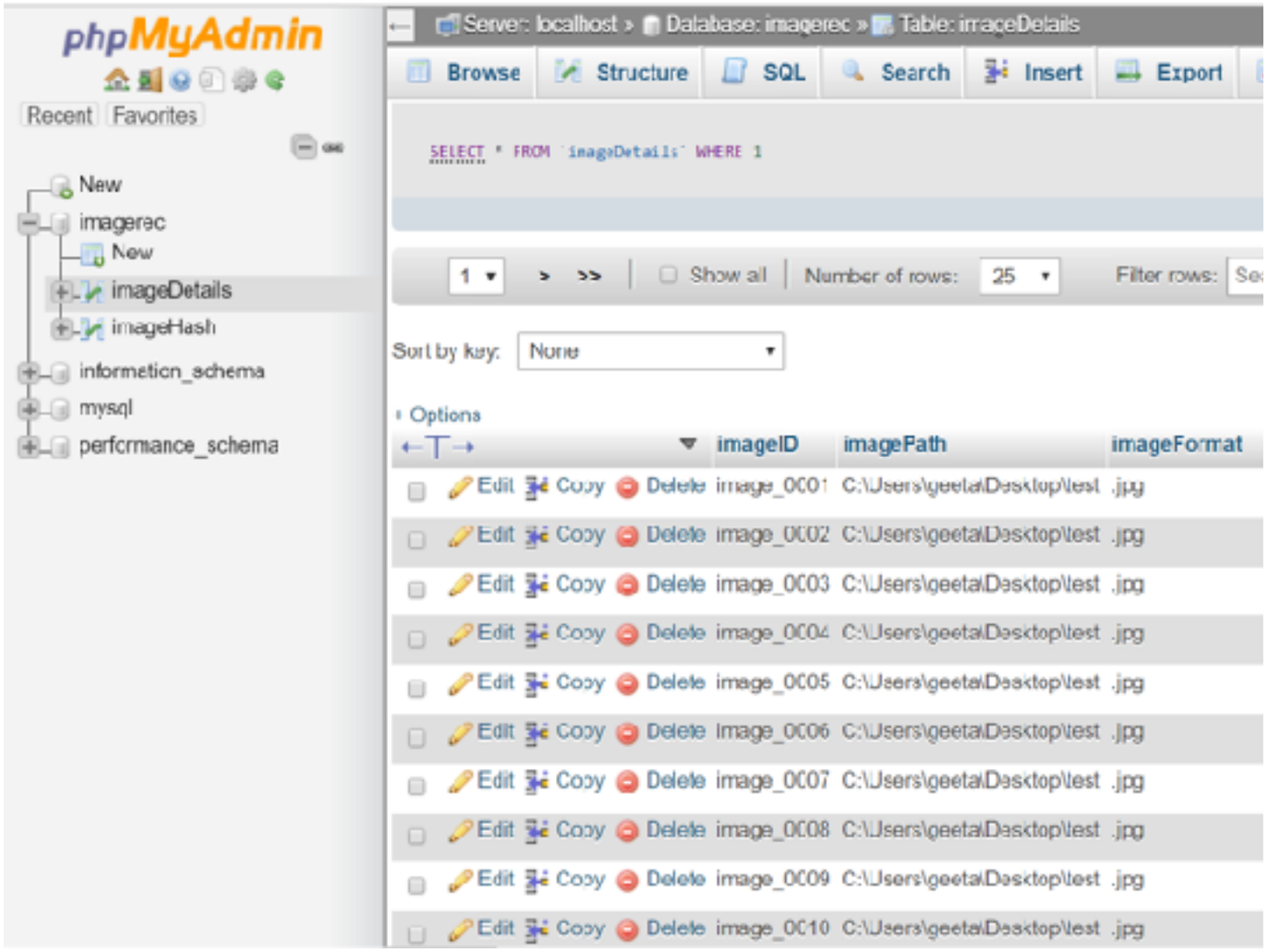
Compute the hash

Speed and Accuracy

- Very few false positives
- Comparison with the other algorithm -Average Hash

Detecting Near-Duplicate images

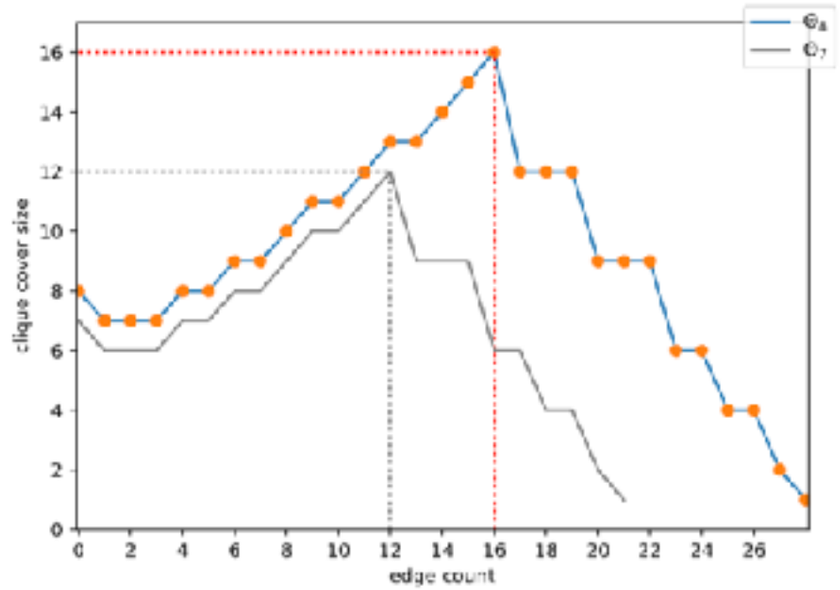
Amazon Web Services

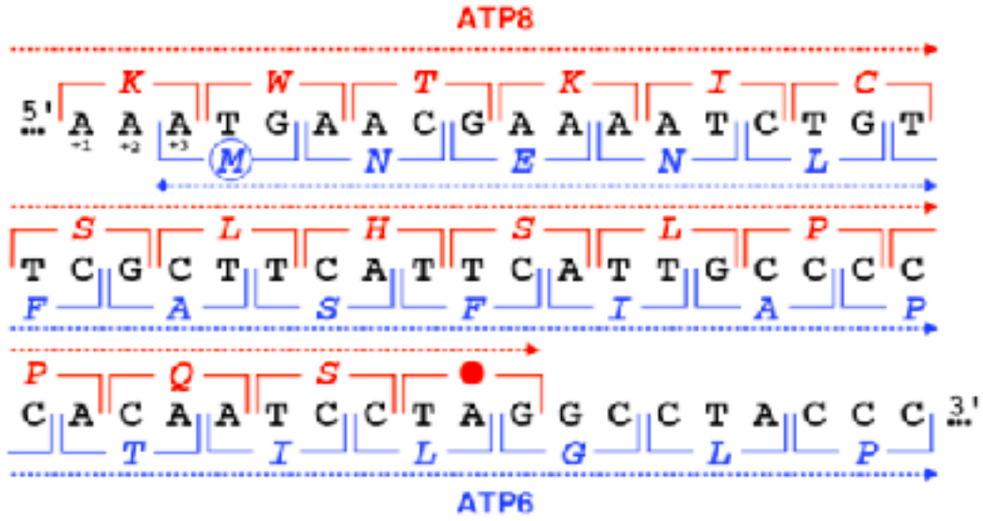


- **Indeterminates**

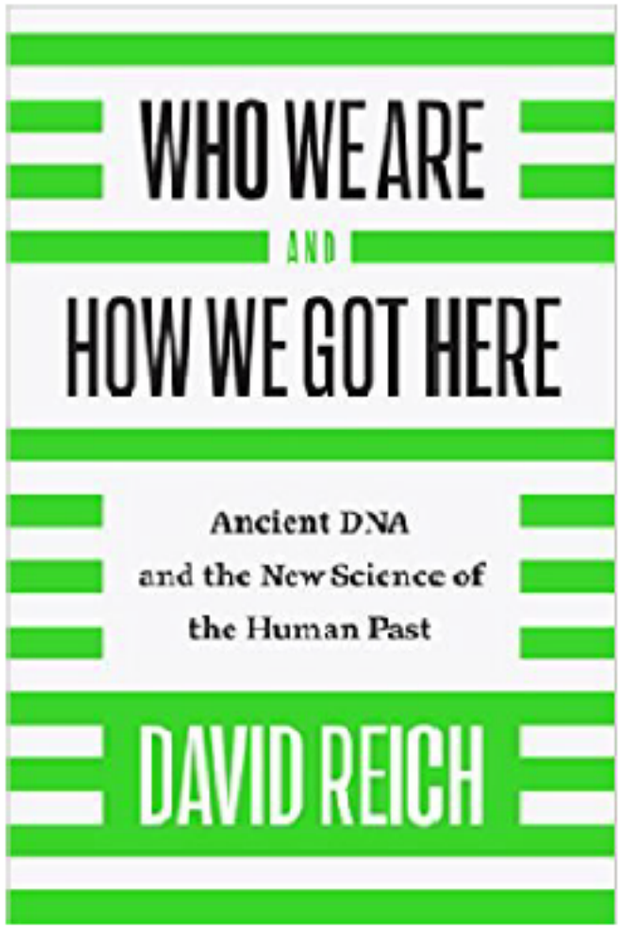
- Ryan McIntyre

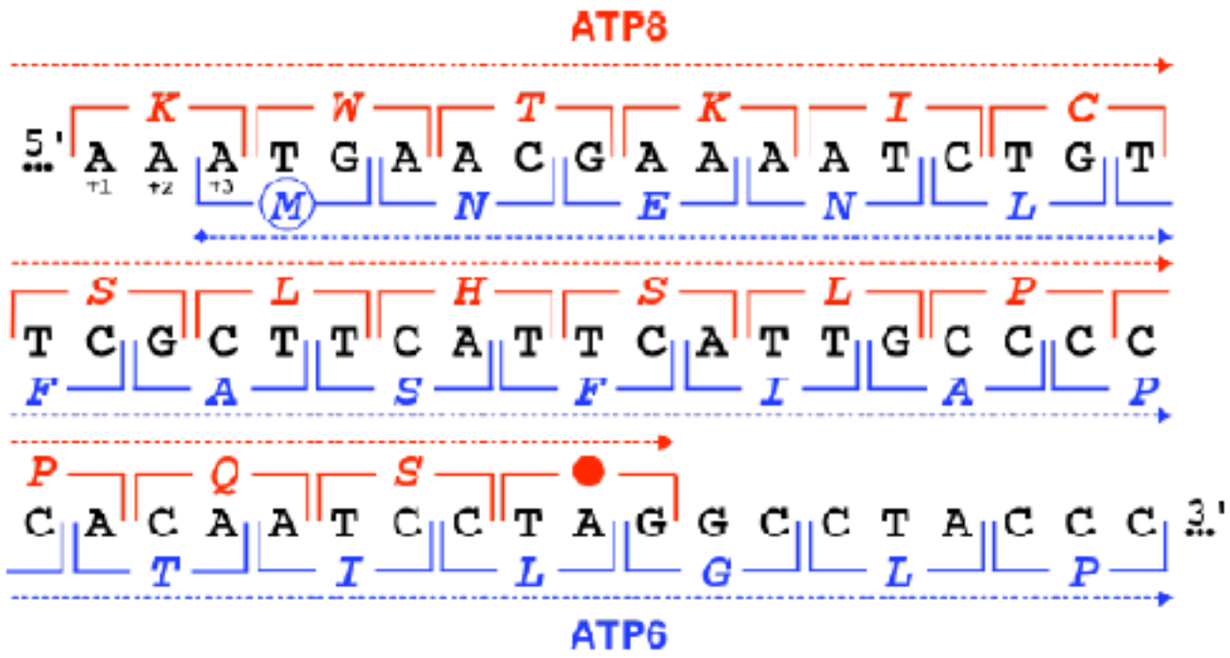
- Algorithms in **bio-informatics**





https://ghr.nlm.nih.gov/gene/MT-ATP6





https://ghr.nlm.nih.gov/gene/MT-ATP6

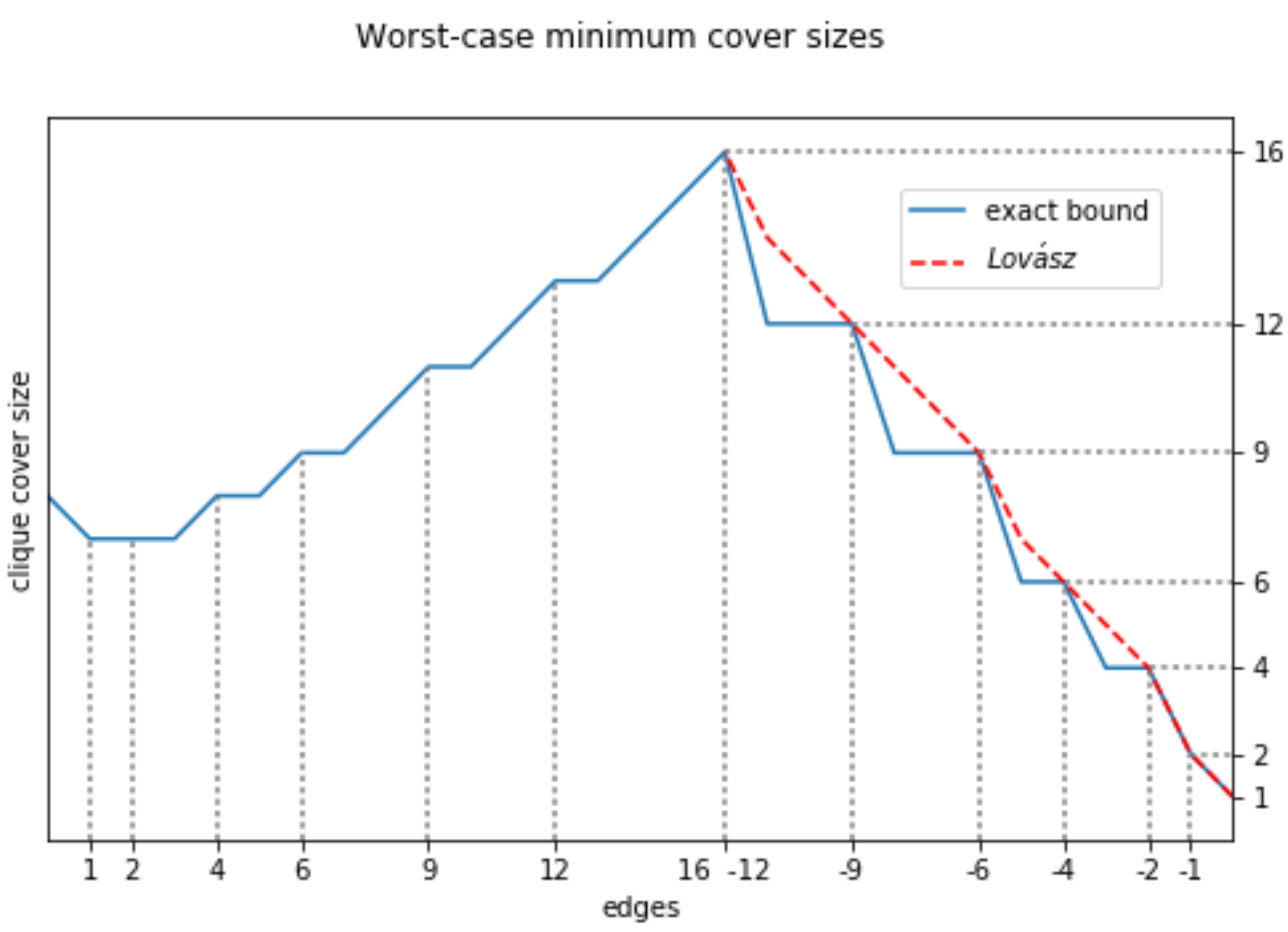
CA{C,A,T}{G,A}TG{A,C}C{T,G,A}AACT

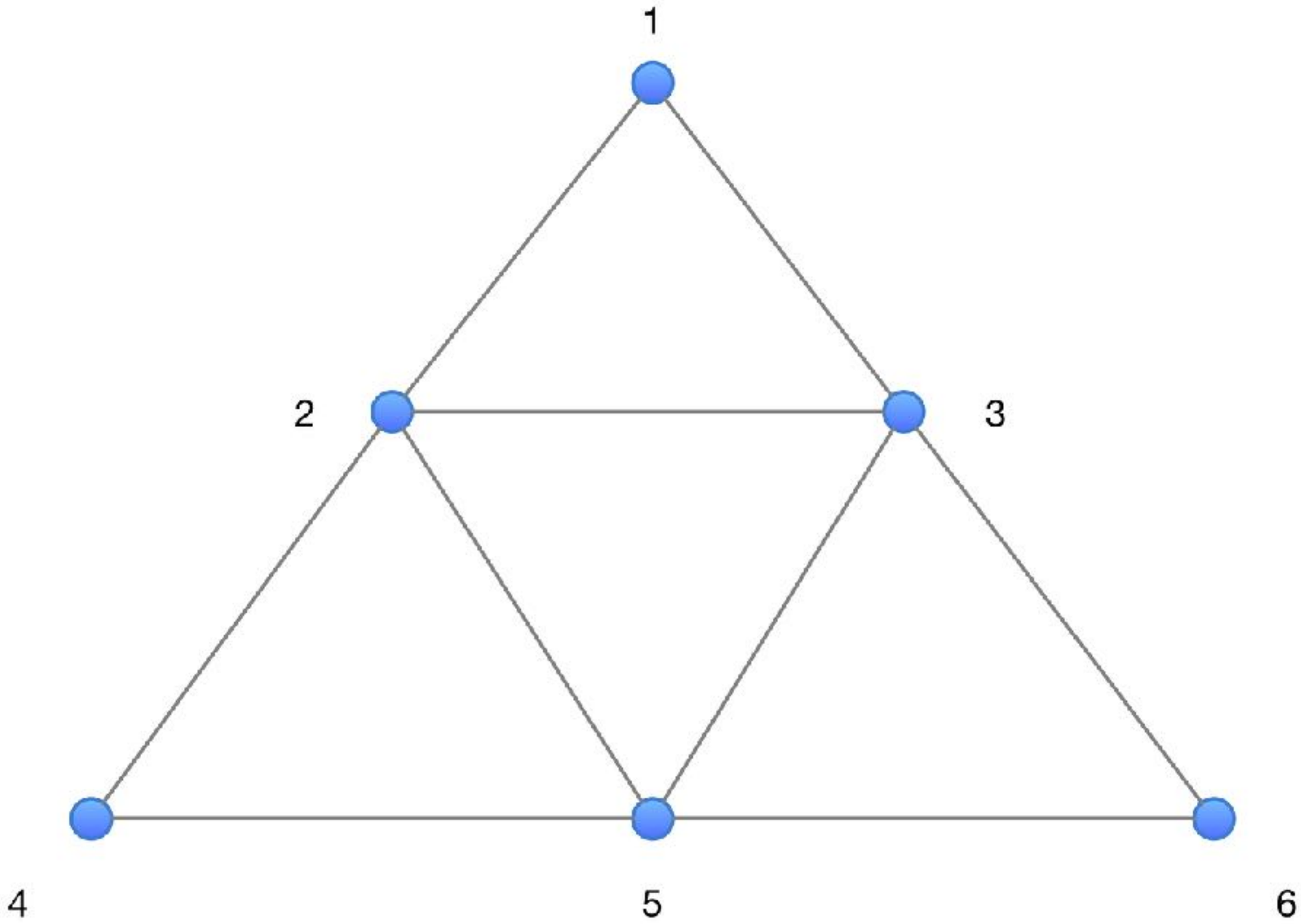
Standing on the shoulders of giants...

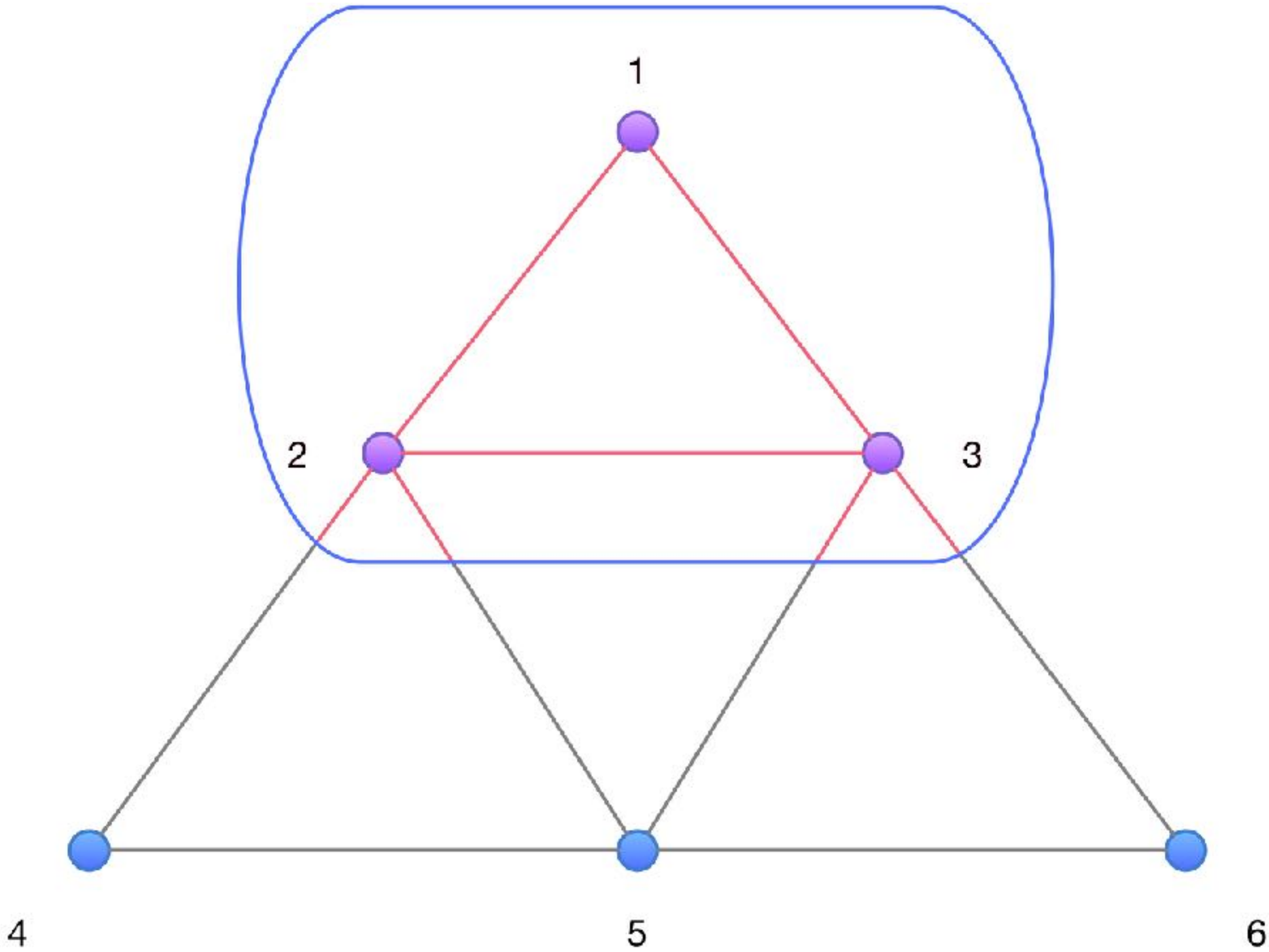
Paul Erdősz
1913–1996

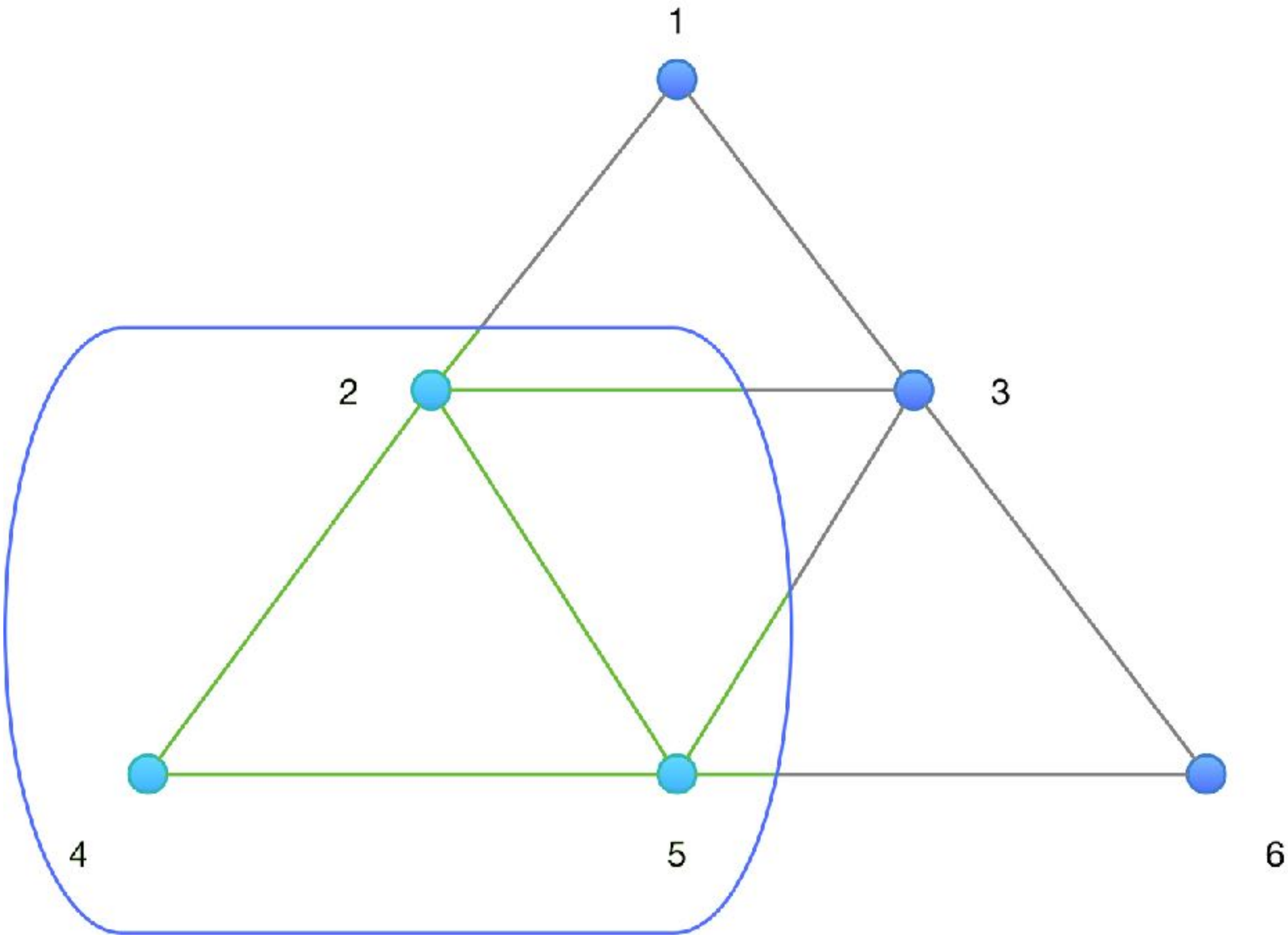
László Lovász
1948–

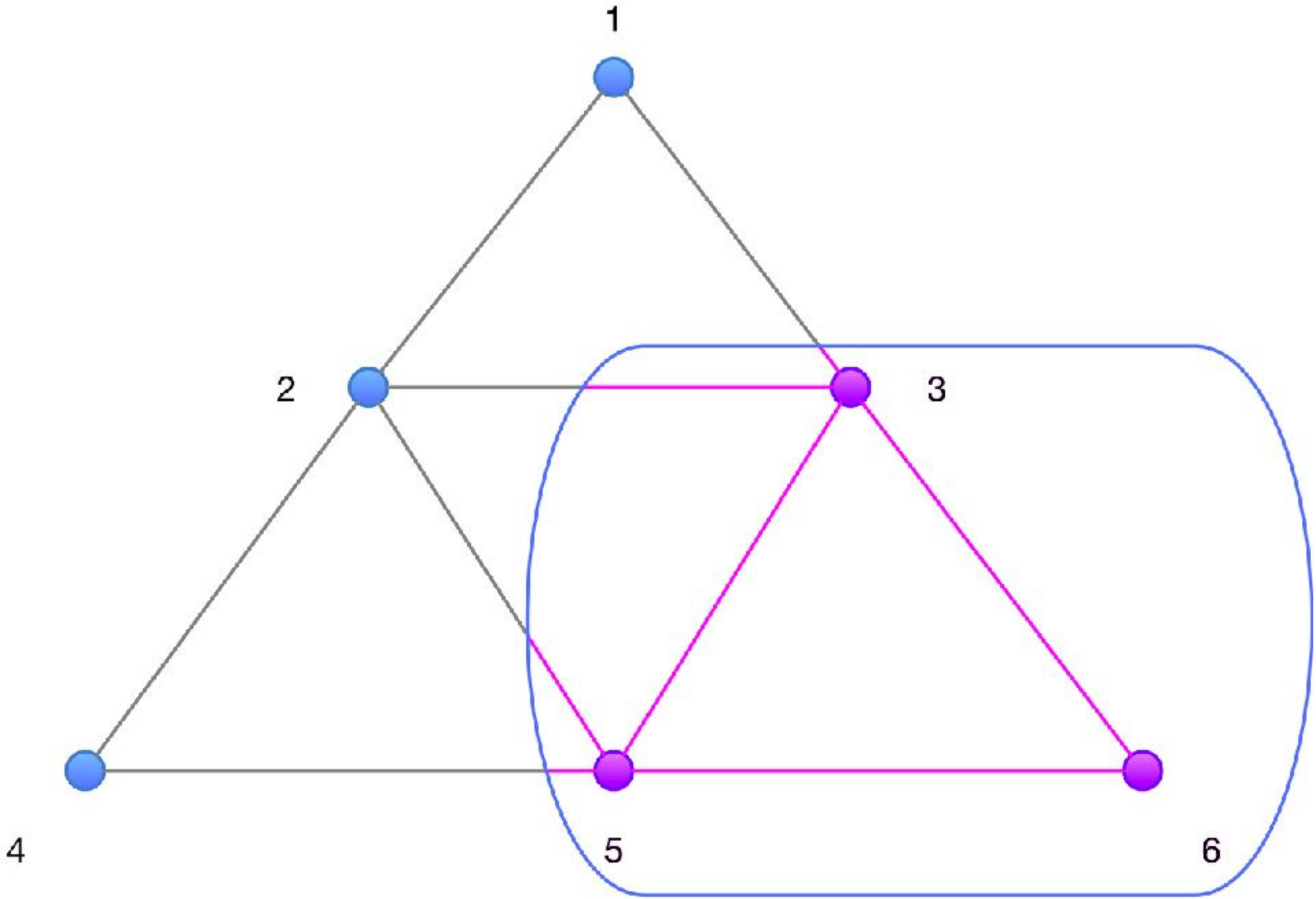
“Keyser Sőze”
1907–?

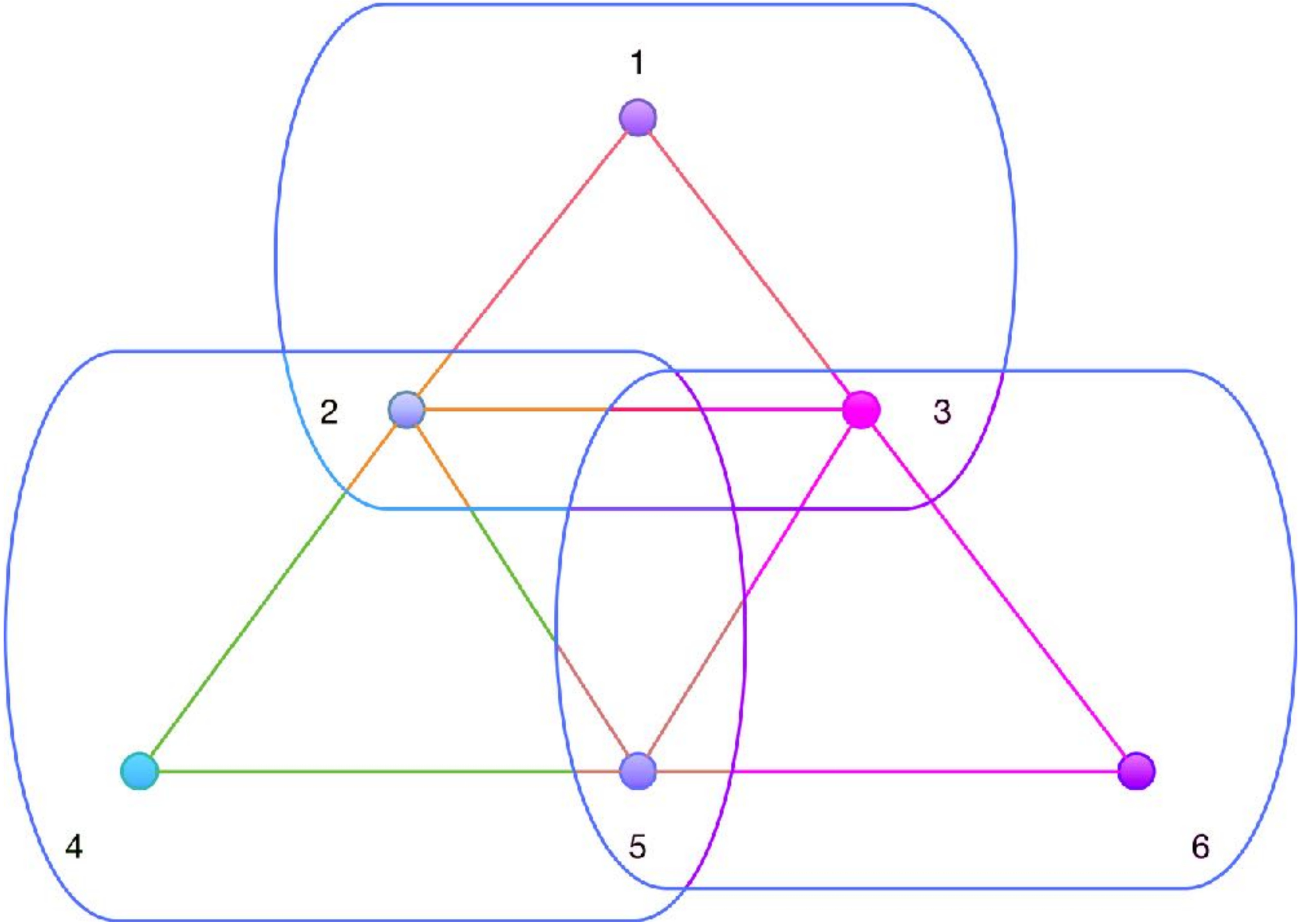

Worst-case minimum cover sizes
clique cover size
edges
exact bound
Lovász
1
2
4
6
9
12
16
-12
-9
-6
-4
-2
-1
16
12
9
6
4
2
1

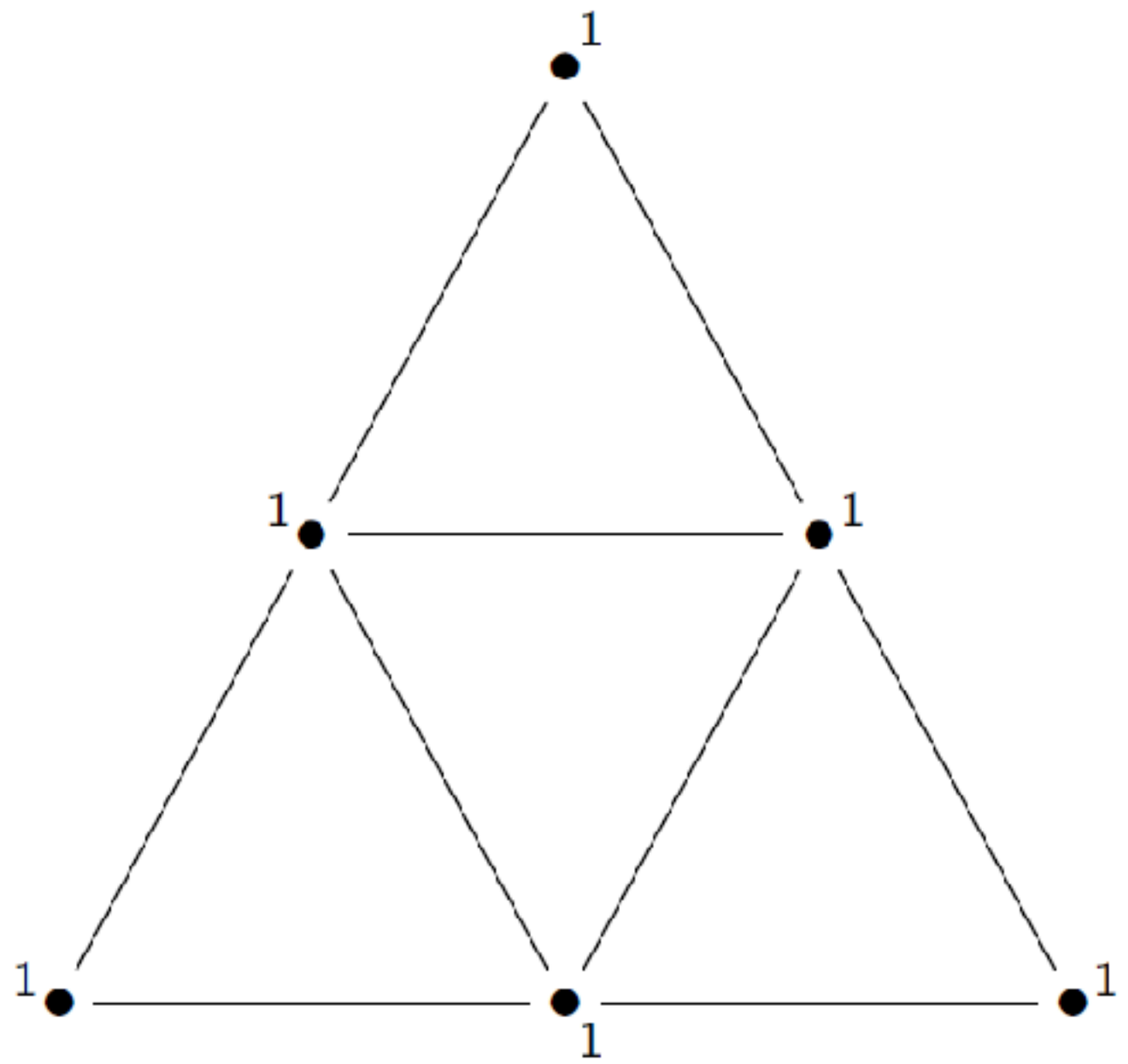

1
2
3
4
5
6

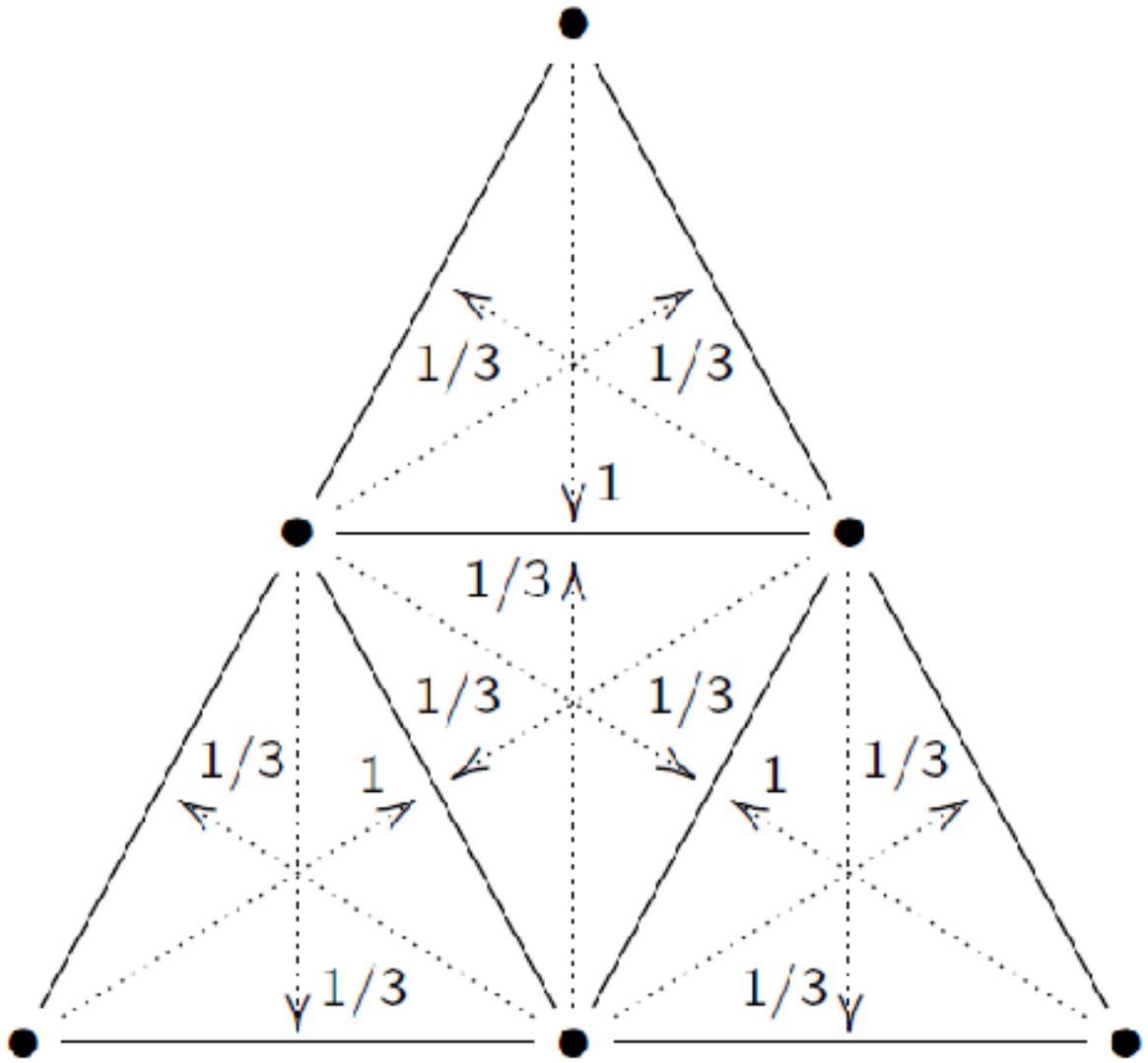

1
2
3
4
5
6

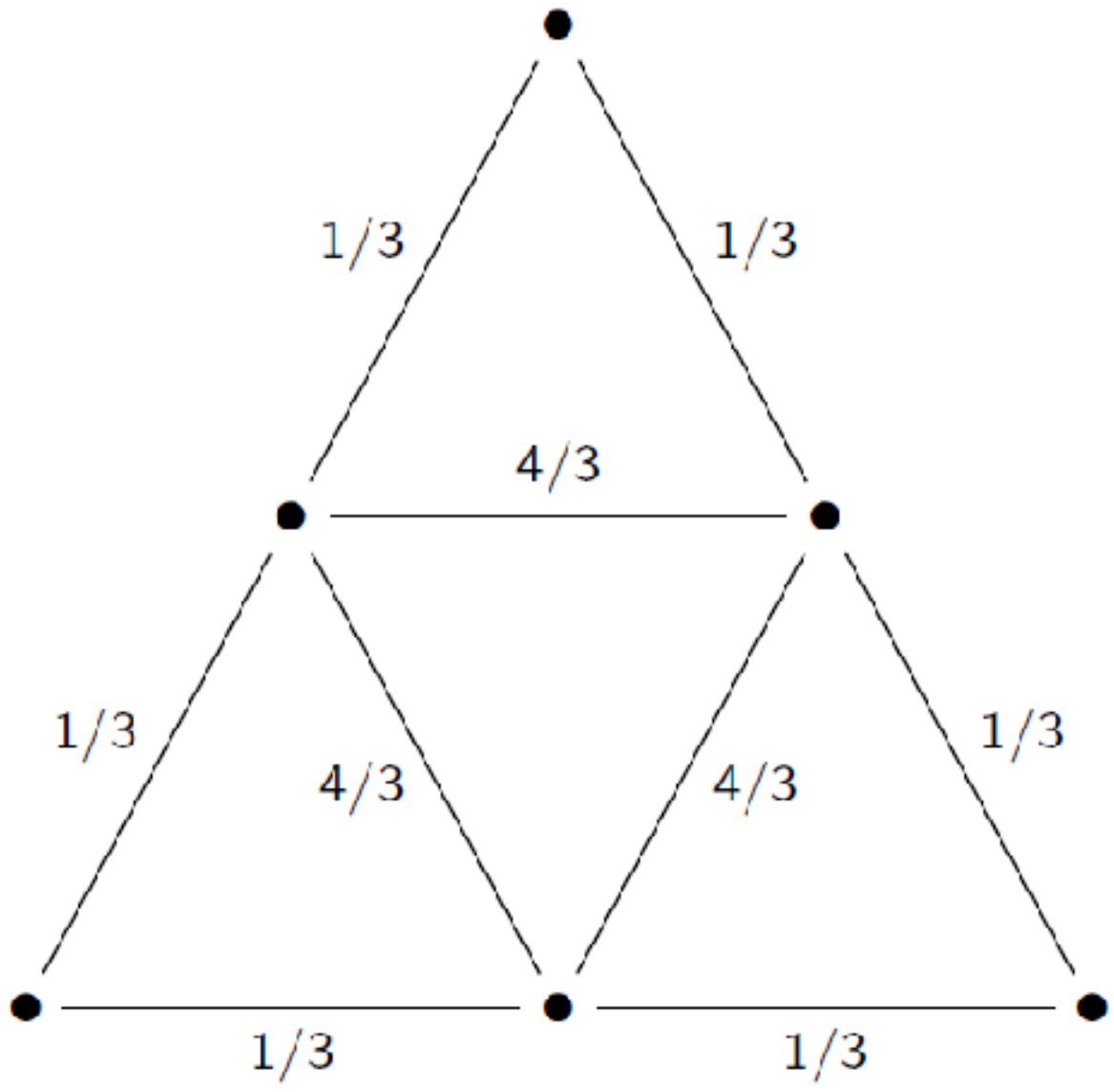

1
2
3
4
5
6

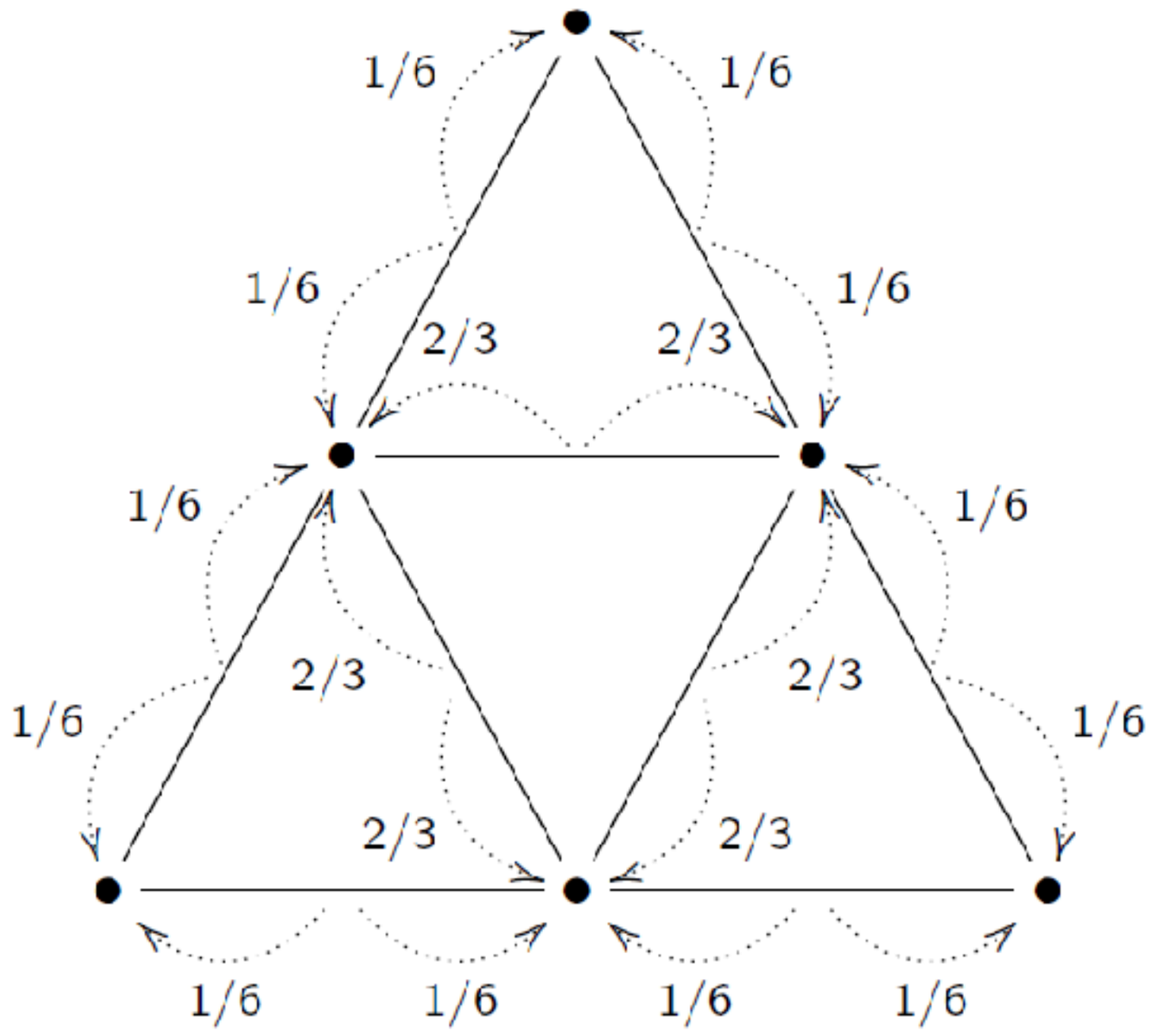

1
2
3
4
5
6

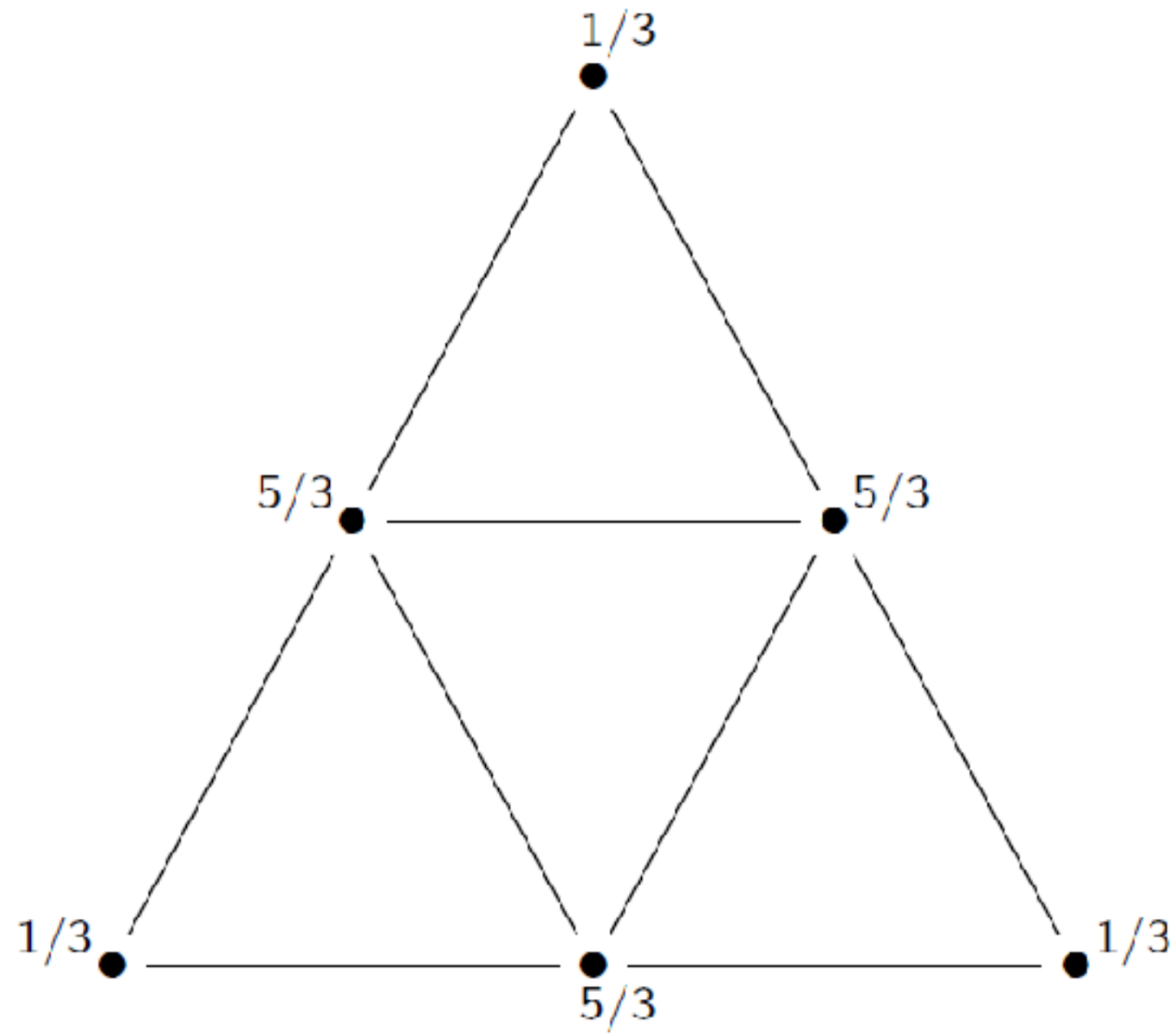

1
2
3
4
5
6

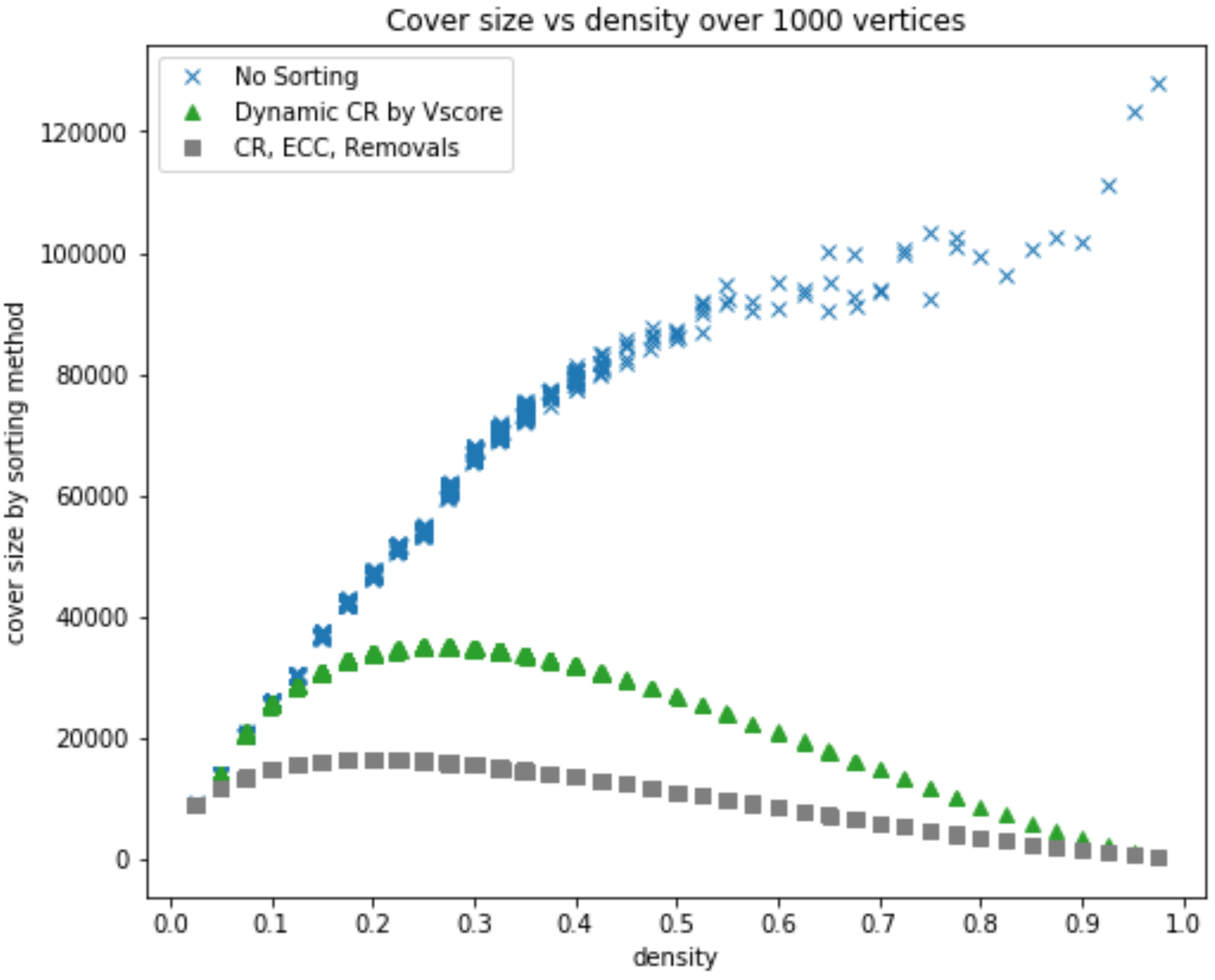

1
1
1
1
1
1


1/3
1/3
1
1/3
1/3
1/3
1
1
1/3
1/3
1/3


1/3
1/3
4/3
1/3
4/3
1/3
4/3
1/3
1/3


1/6
1/6
1/6
1/6
2/3
2/3
1/6
1/6
2/3
2/3
1/6
1/6
1/6
1/6


1/3
5/3
5/3
1/3
1/3
5/3


Cover size vs density over 1000 vertices
No Sorting
Dynamic CR by Vscore
CR, ECC, Removals
cover size by sorting method
120000
100000
80000
60000
40000
20000
0
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
density

http://bit.ly/Cyber-CI-2018

Michael Soltys michael.soltys@csuci.edu
Zane Gittins zane.gittins561@myci.csuci.edu
Eric Gentry eric.gentry045@myci.csuci.edu
Geetanjali Agarwal geetanjali.agarwal004@myci.csuci.edu
Ryan McIntyre ryan.mcintyre466@myci.csuci.edu