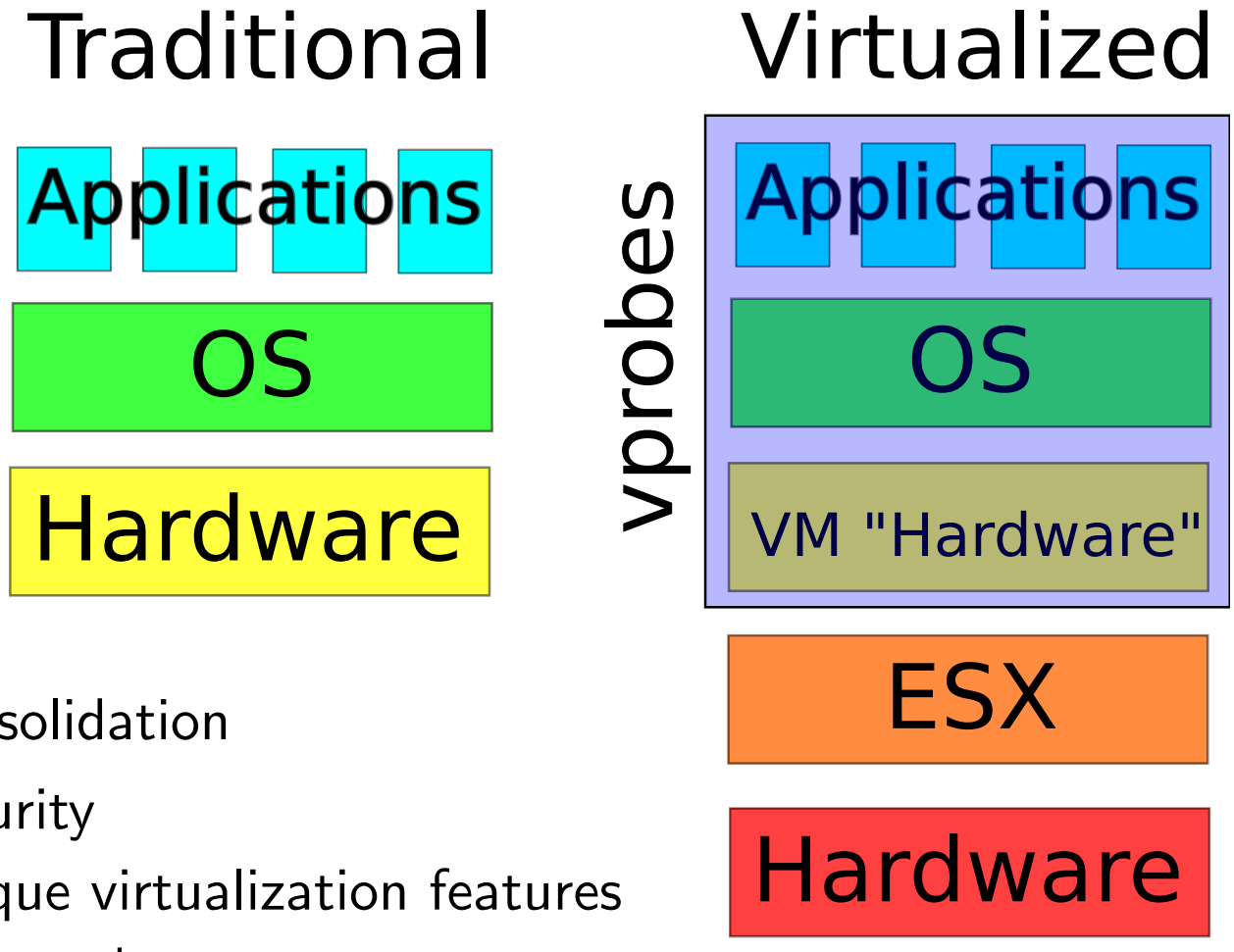
Possible application: Proof of identity

- Numerous cases where you want to prove who you are
- Example: authorize a credit card transaction
- Don't want stores to be able to charge you for more stuff later
- Use zero-knowledge proof to prove who you are, instead of a credit card number you keep secret

Virtualization



- Consolidation
- Security
- Unique virtualization features
  - vprobes

Idea of the construction of $\mathbf{p}_k(n)$, cont

Let $f(n,k)$ be the probability that $k \mid (a+b)$ and $(b+c)$ for a random *abc*-permutation of length n.

Lemma (Pak-Redlich, 2008)

$$f(n,k) = \begin{cases} \frac{\left(\frac{n}{k}+1\right)\left(\frac{n}{k}+2\right)}{(n+1)(n+2)} & \text{if } k \mid n \\ \frac{\lfloor \frac{n}{k} \rfloor \left(\lfloor \frac{n}{k} \rfloor + 1\right)}{n(n+1)} & \text{if } k \nmid n. \end{cases}$$

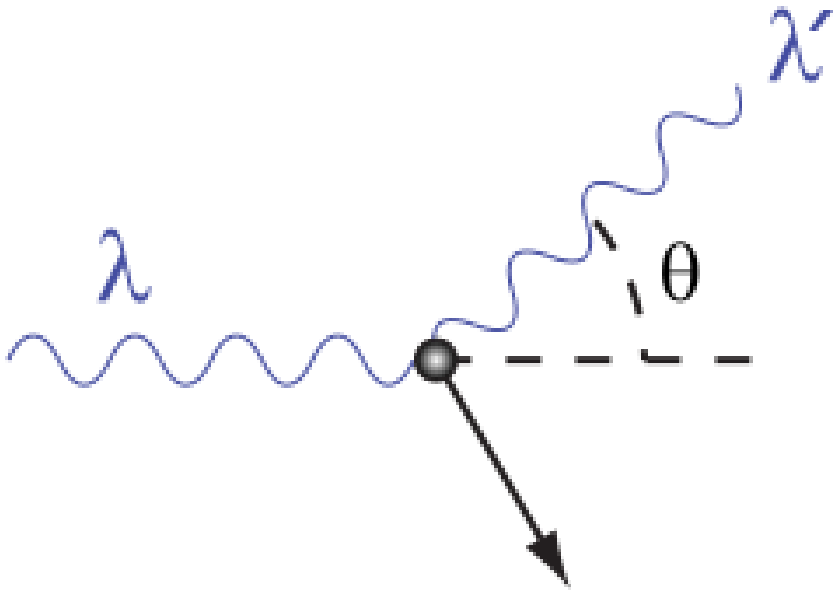
PLAYING IN THE SANDBOX

David Benjamin

Process Isolation in Google Chrome

Compton Scattering Theory

- Billiard-ball style collisions
- Relativistic energy: $E^2 = p^2c^2 + m^2c^4$



$$\Delta\lambda = \frac{h}{mc}(1 - \cos\theta)$$

Calculating the Cross-Section

- Uniform gas density $\rightarrow$ constant scattering probability for a fixed distance

$$I = I_0 \, e^{-\frac{L}{\lambda}}$$

$$\frac{1}{\lambda} = n\sigma$$

$$\sigma(V) = \frac{1}{nL} \ln\left[\frac{I_0(V)}{I(V)}\right]$$

Amplitude Results

- Classically-expected increase for large θ not observed
- Large systematic errors
  - Unusually weak signal at 30° — likely discriminated against
  - Scintillator efficiency
  - Detector drift
- Errors too significant to verify Klein-Nishina; however data definitely inconsistent with Thomson model

Idea of the construction of $\mathbf{p}_k(n)$

Let A_k be the event that $k|(a+b)$ and $(b+c)$, and let B_k be the event that $(a+b)/k$ and $(b+c)/k$ are relatively prime integers. Then

$$\mathbf{p}_k(n) = Pr(A_k) \cdot Pr(B_k \text{ given } A_k)$$

Explanations–Classical and Quantum

In 1887 Hertz observes a new phenomena

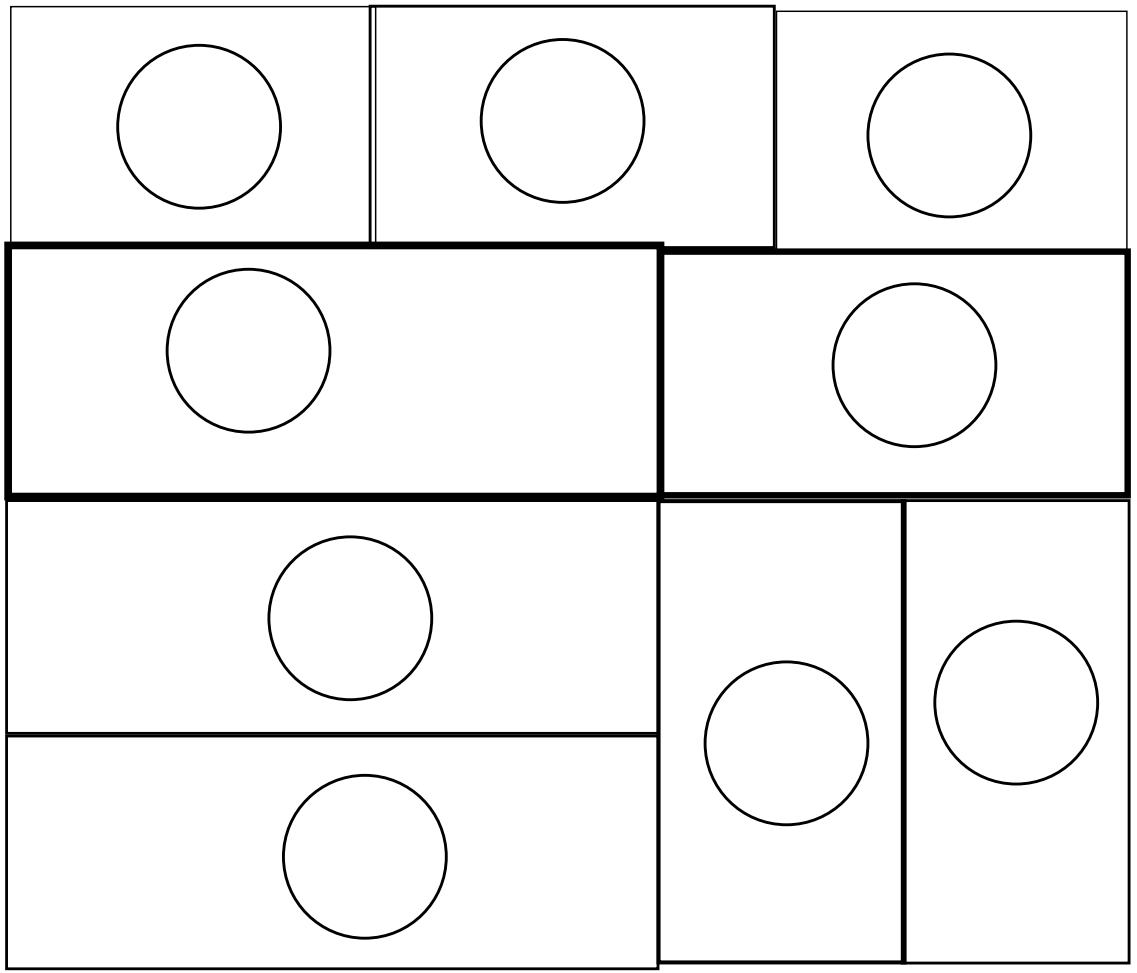
No classical explanation exists

In 1905 Albert Einstein proposes a quantum explanation

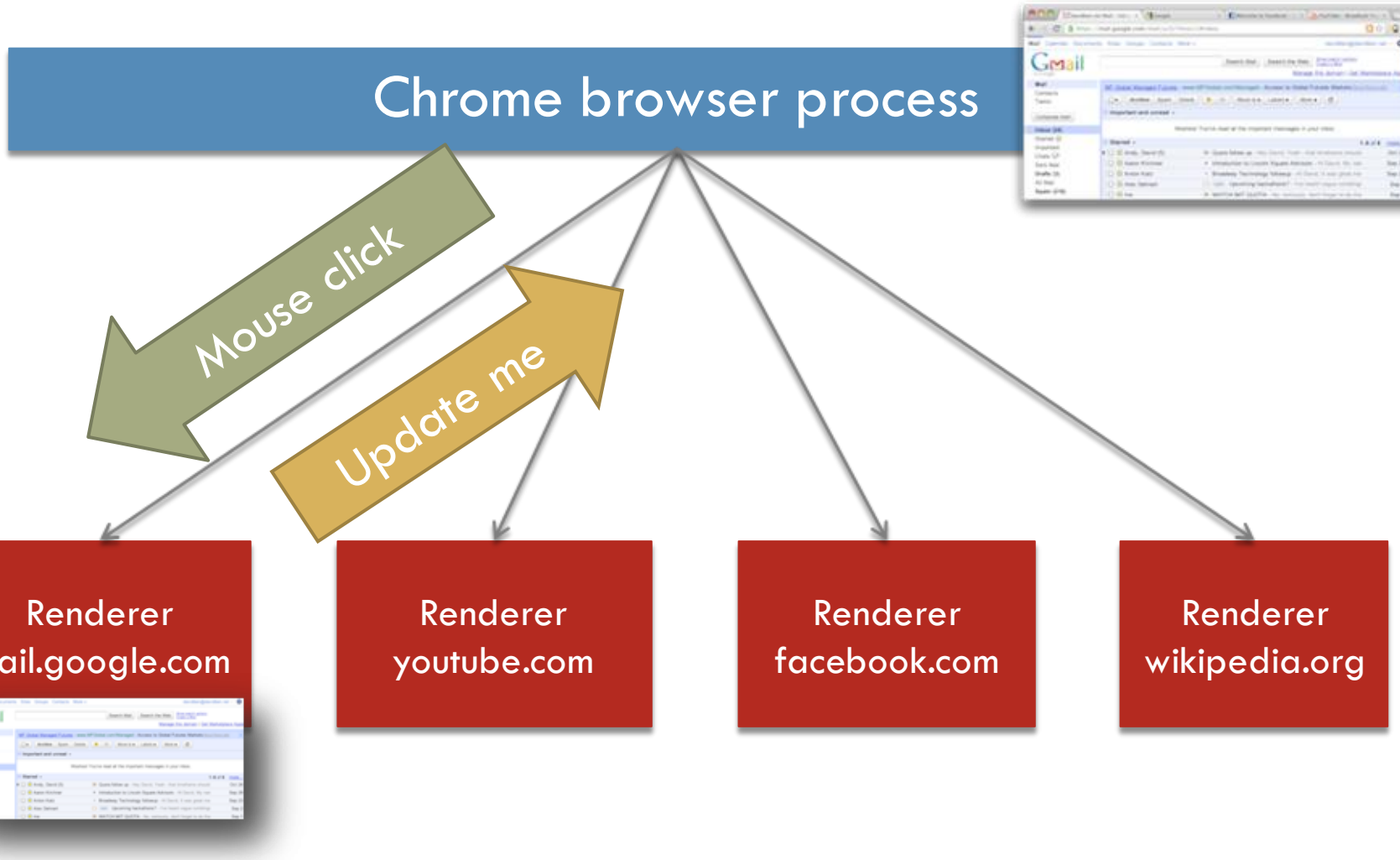
$$E_{photon} = h\nu \qquad KE_{max} = h\nu - \Phi$$

Map coloring ZKP

Commit



Multi-process browsing



Goal

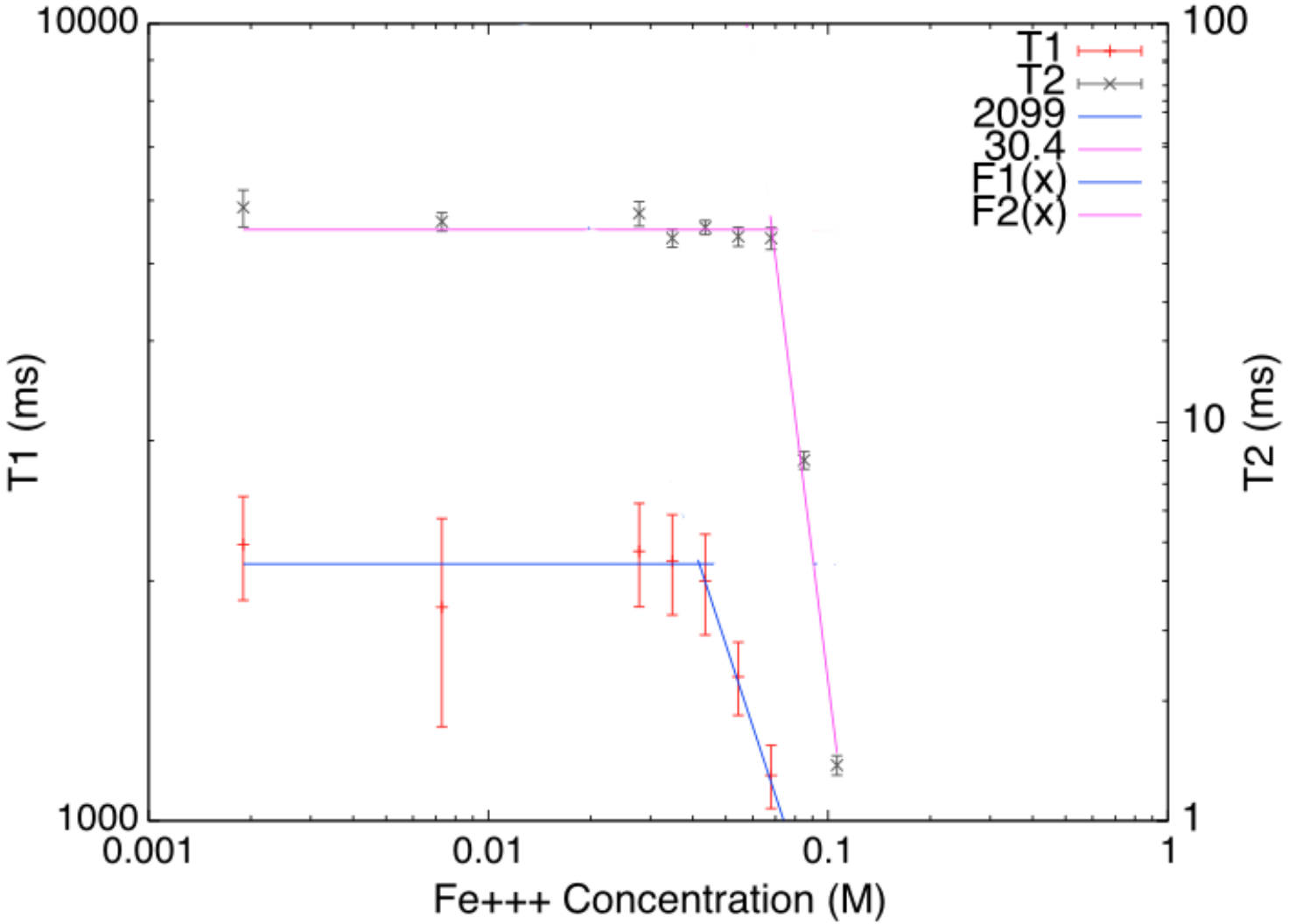
Provide an intrusion detection system that is robust against attacks from malware, by leveraging vprobes to run the agent on the host

Electron–Xenon Scattering: The Ramsauer-Townsend Effect

Daniel J. Fremont

8.13
Massachusetts Institute of Technology

Effect of Fe^{3+} Ions on T1 and T2



T_1 slope = -1.3 ± 0.4

T_1 $\chi_r^2 = 0.07$

T_2 slope = -6.9 ± 0.2

T_2 $\chi_r^2 = 12$

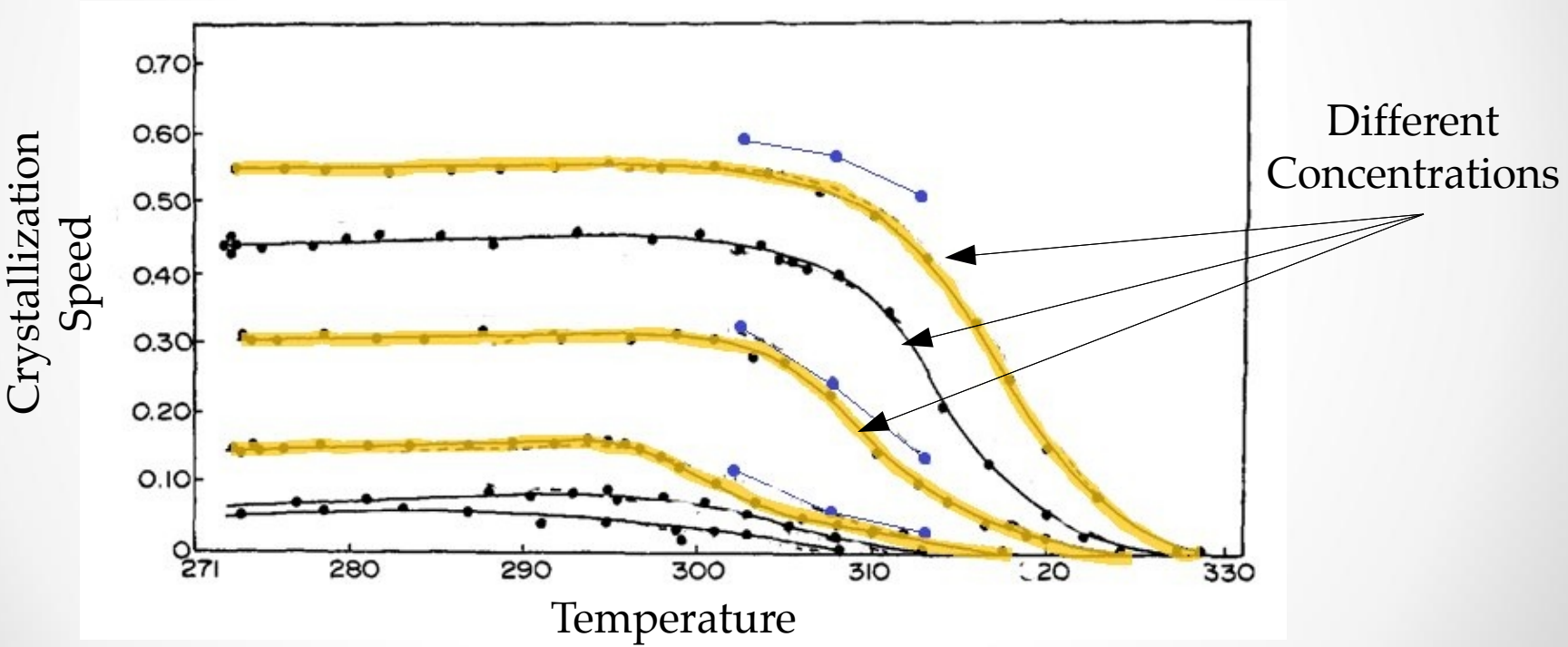
Cost of Intrusions

$114 billion	Total global cost of cybercrime annually, as estimated by Symantec
$75 billion	2011 spending on IT security for US companies, according to the Ponemon Institute
$170 million	Cost to Sony of the recent PlayStation Network hack, including shutting down PSN, network security improvements, etc.

Sources: The Fiscal Times, Huffington Post

Previous Work

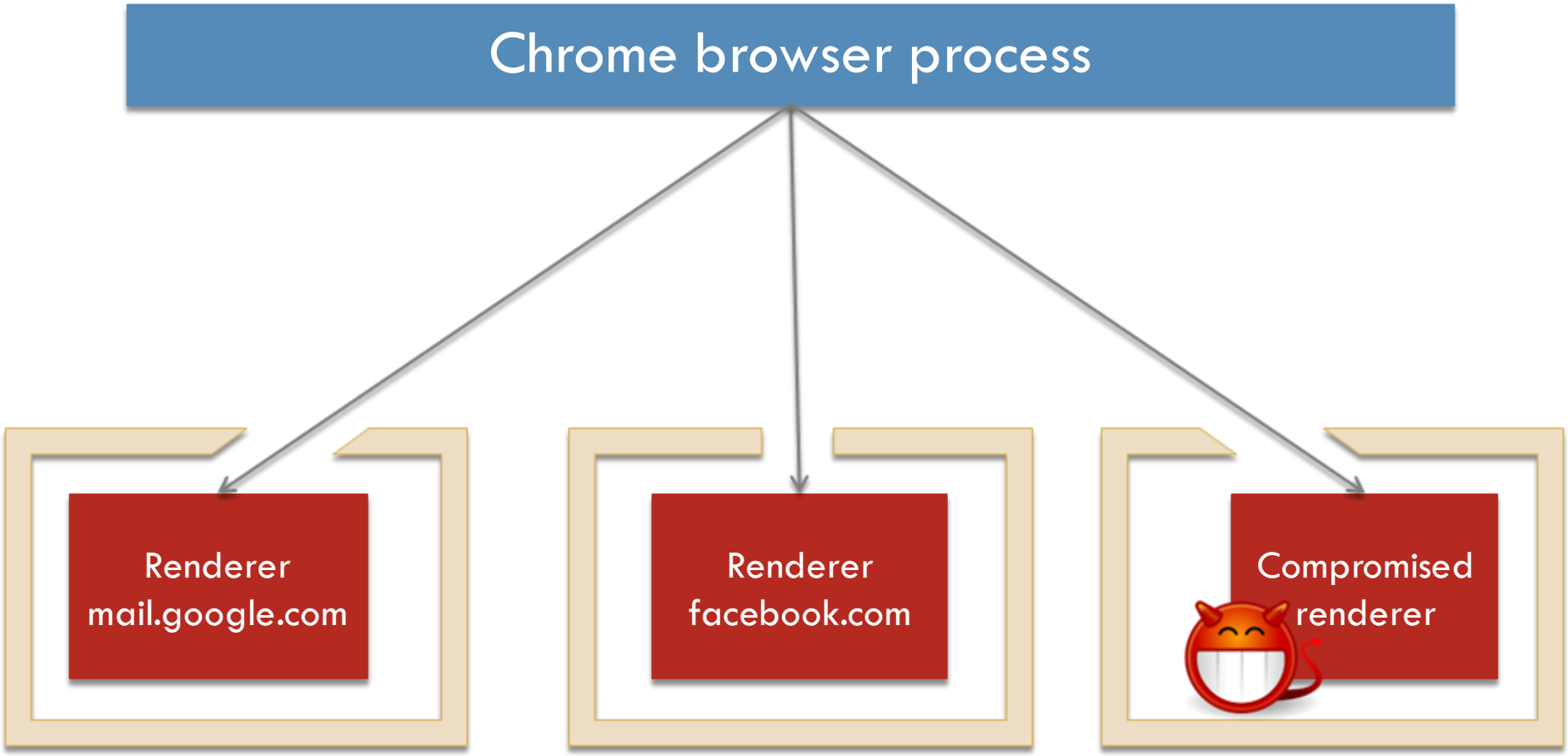
- Dietz, Bruckner, and Hollingsworth (1957)



Timeline

Week 1	Get set up at VMware again
Week 2	Re-familiarize with vprobes
Week 3	Find off-the-shelf exploits for Apache and other services
Week 4	Write a custom Apache exploit
Week 5	More exploit-writing
Week 6	Review literature on intrusion detection again; begin writing analyzer (e.g., finite automata)
Week 7	Continue literature-based analyzer
Week 8	Start custom analyzer (e.g., SVM)
Week 9	Continue custom analyzer
Week 10	Code cleanup and begin code review
Week 11	Finish code review; begin writing report
Week 12	Finish writing report

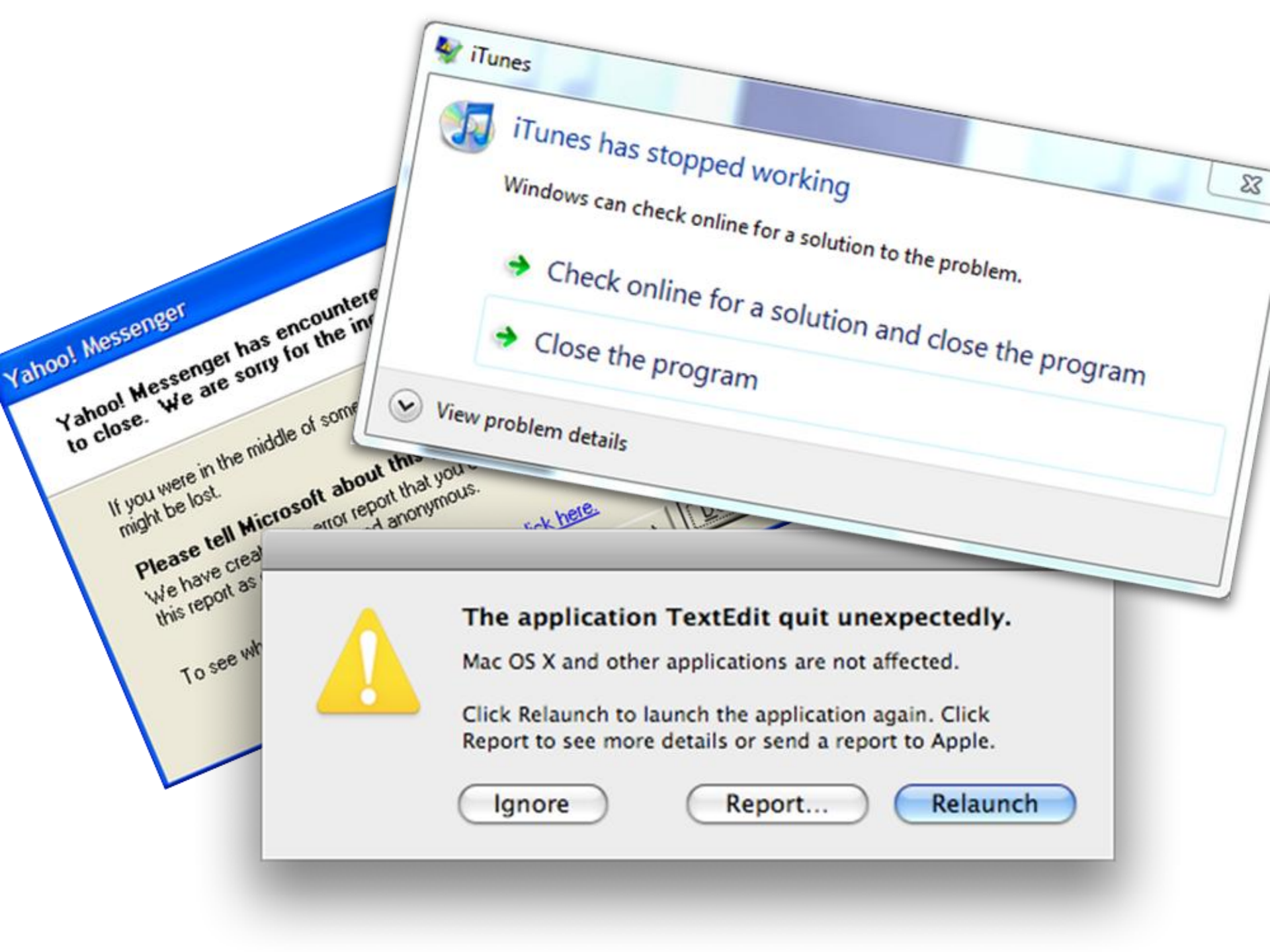
Enforcing security



Systematic Error

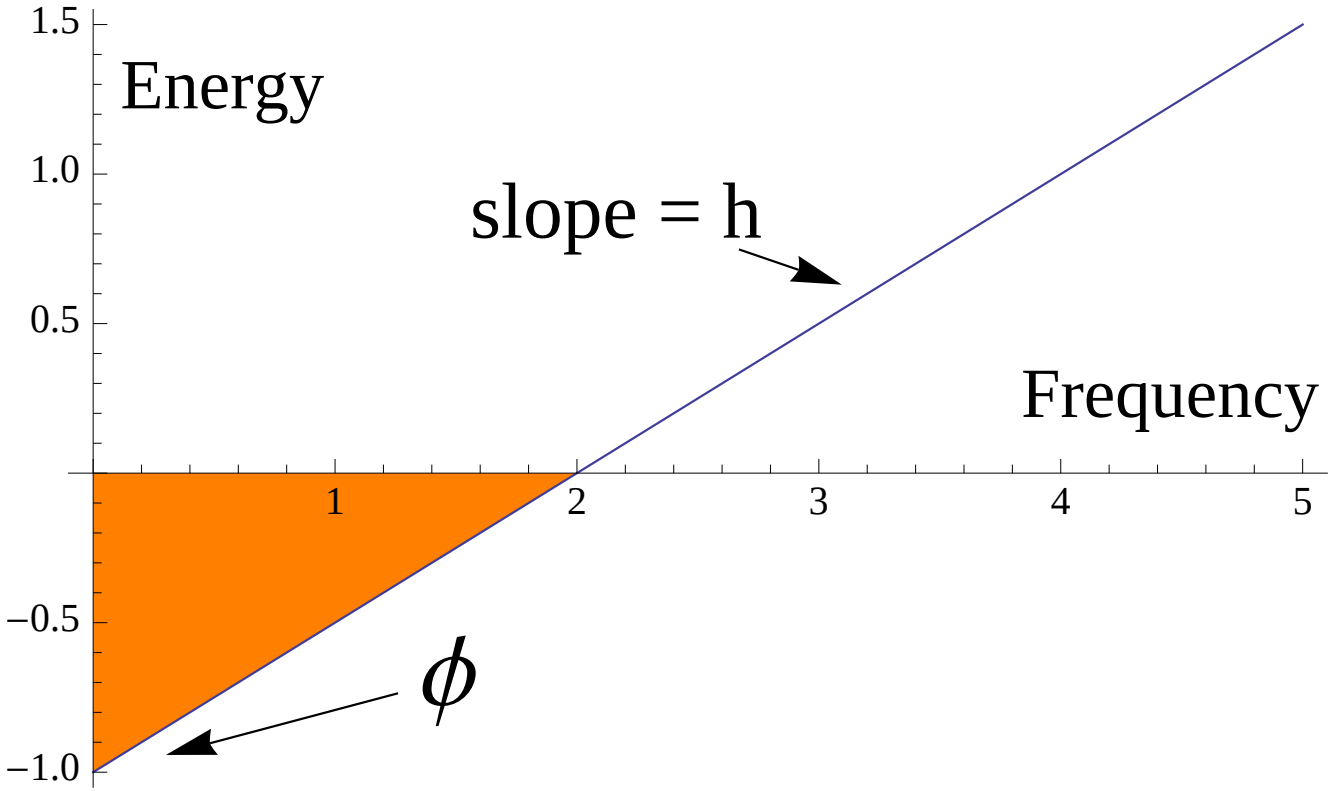
Potassium build up on the anode causes reverse photoelectric currents

Insufficient Higher Voltage Data

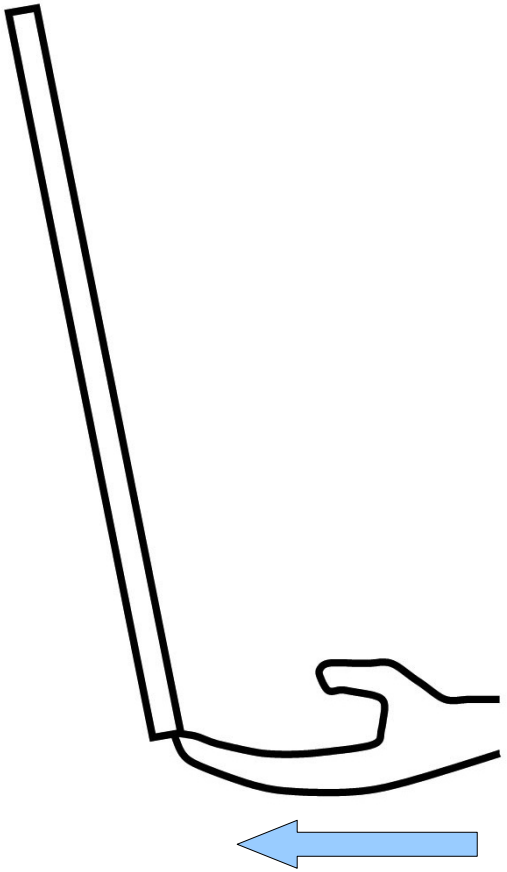

Yahoo! Messenger
Yahoo! Messenger has encountere
to close. We are sorry for the in
If you were in the middle of some
might be lost.
Please tell Microsoft about this
We have creat
this report as
To see wh
error report that you
d anonymous.
ick here.
iTunes
iTunes has stopped working
Windows can check online for a solution to the problem.
Check online for a solution and close the program
Close the program
View problem details
The application TextEdit quit unexpectedly.
Mac OS X and other applications are not affected.
Click Relaunch to launch the application again. Click Report to see more details or send a report to Apple.
Ignore
Report...
Relaunch

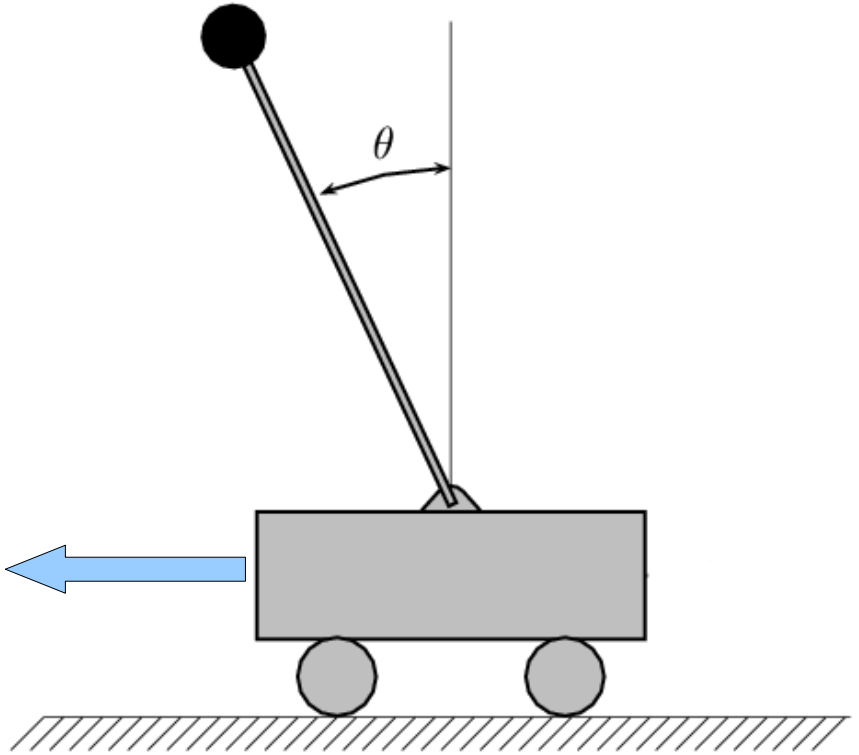
Einstein's theory

$$KE_{e^-} = h\nu - \phi$$



Unstable systems

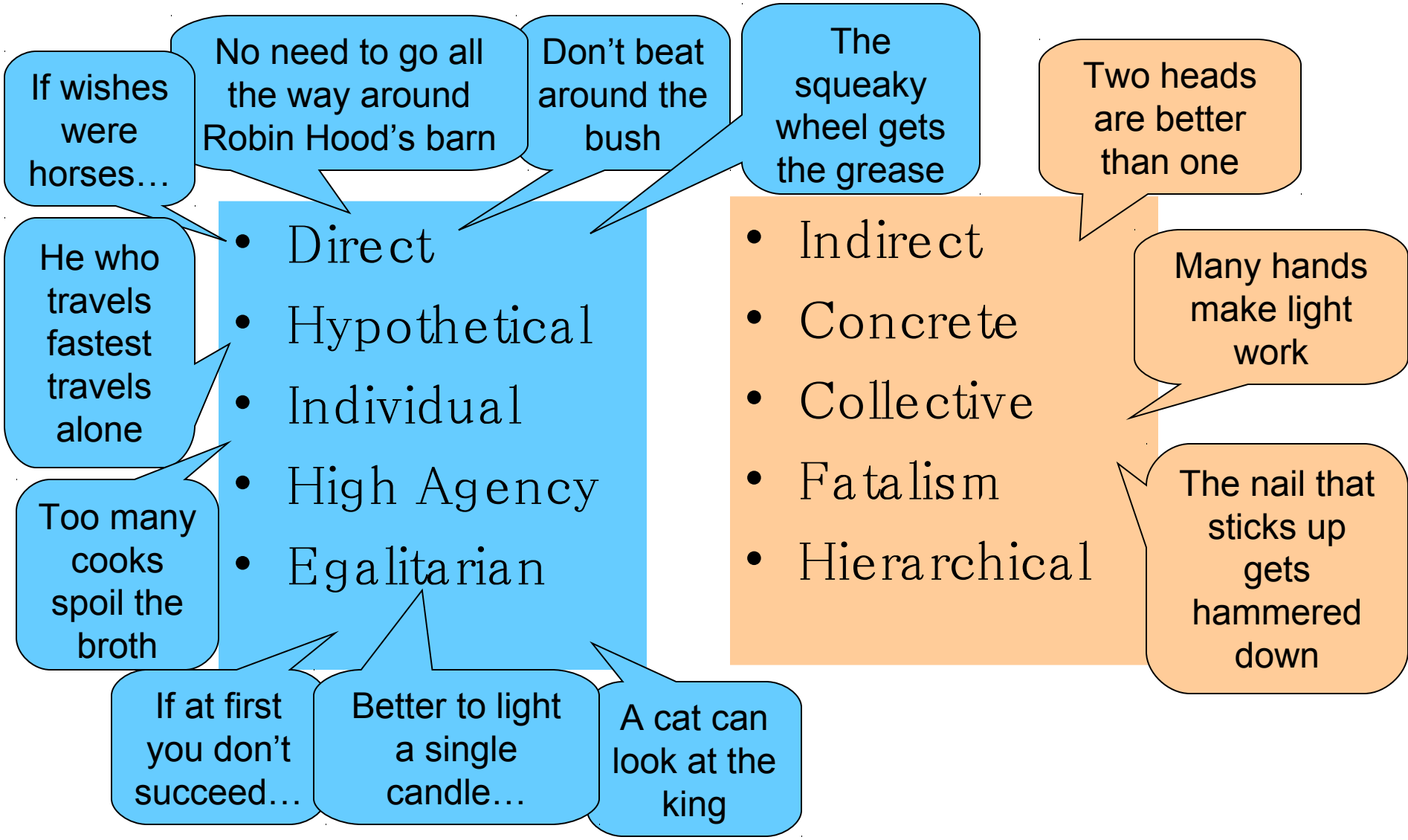




Spin-Spin Relaxation (T2)

- Loss of phase coherence
- Interactions between nearby spins

Culture and Persuasion



Longer phrases, up to a limit

Professor McGonagall…

- was 5.5%
- and 4.2%
- had 3.4%
- said 2.7%

McGonagall was…

- now 6.1%
- hurrying 6.1%
- looking 6.1%
- right 6.1%

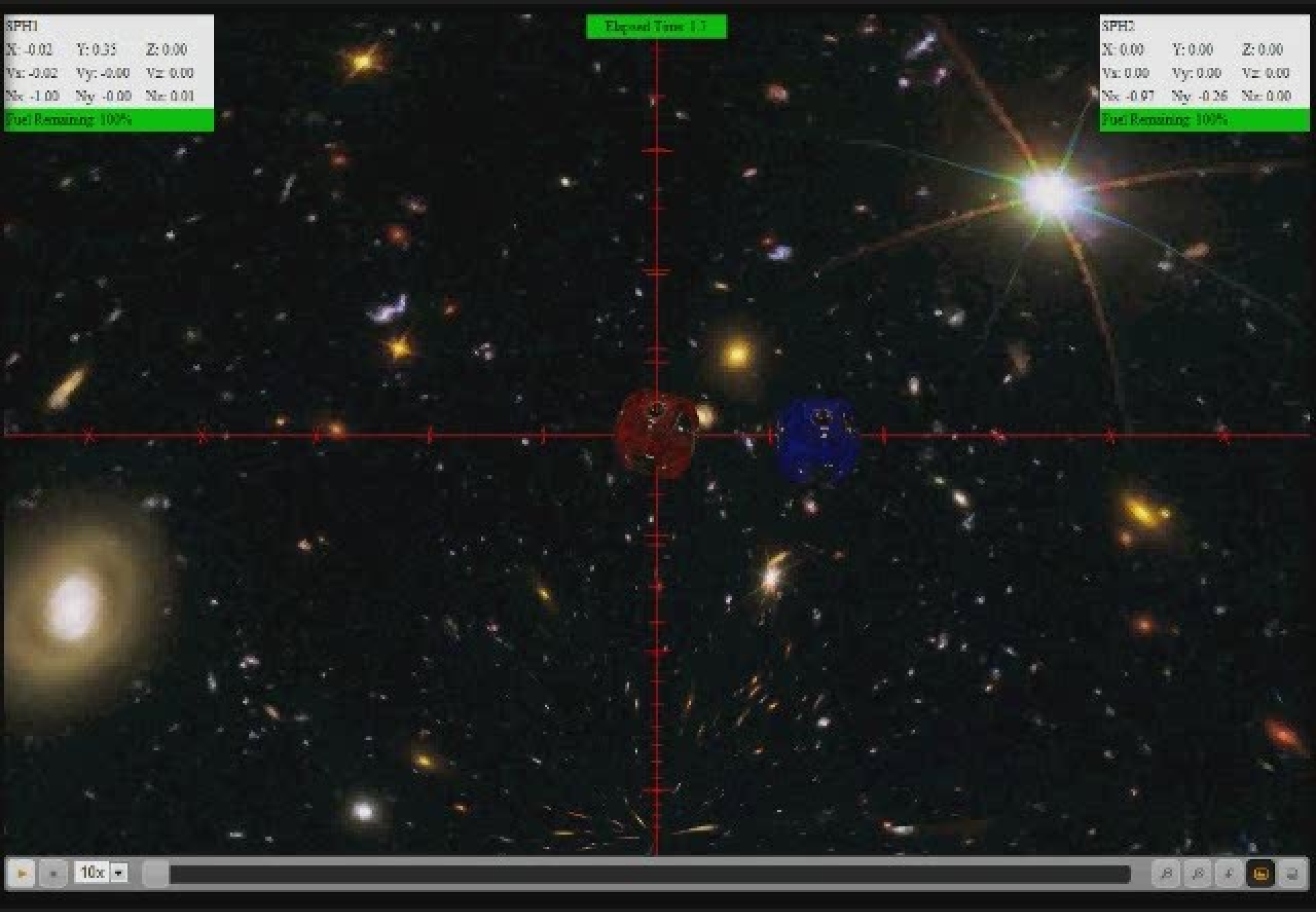
Professor Flitwick burst into flames and curled up, purring deeply. The common room emptied as people drifted off to bed. he went into the thick black trees.

Harry Potter and the Wide-Screen

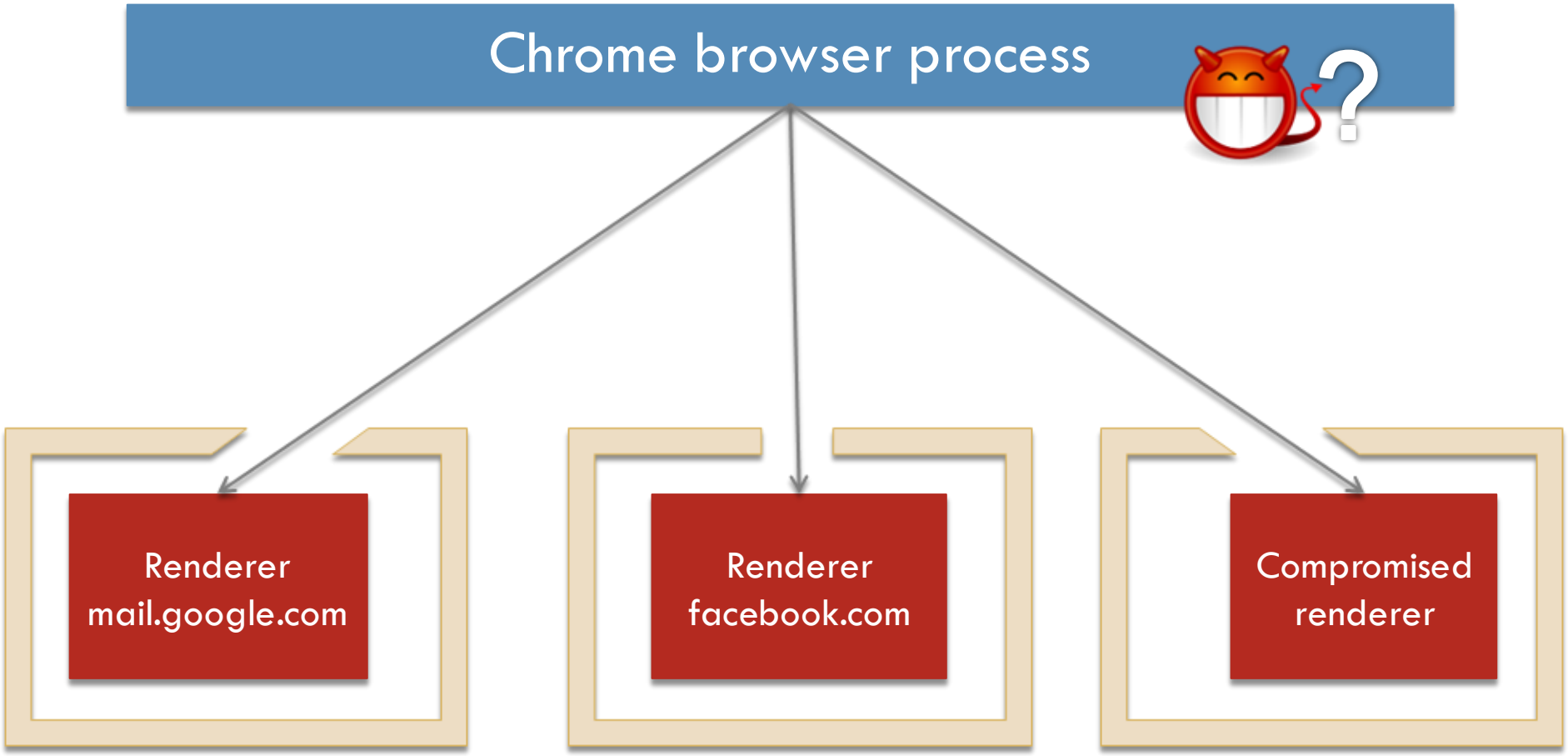
Work required

- vprobe script to get syscall information from the kernel (Summer 2011)
- Build analysis modules (begun Summer 2011)
- Build up collection of exploits and normal behaviors to test against

Scrapbook (PSP)

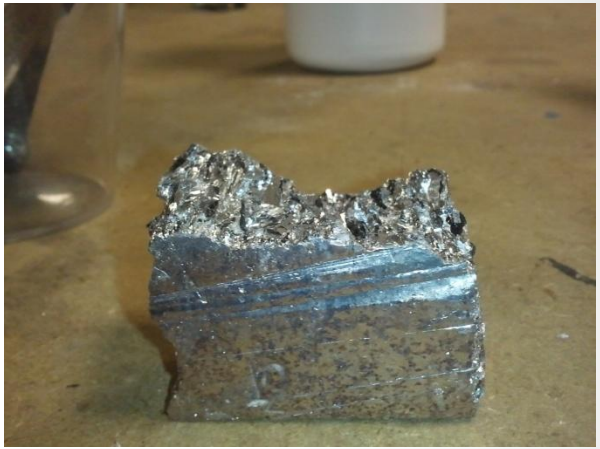

SPH1
X: -0.02 Y: 0.35 Z: 0.00
Vx: -0.02 Vy: -0.00 Vz: 0.00
Nx: -1.00 Ny: -0.00 Nz: 0.01
Fuel Remaining: 100%
Elapsed Time: 1.7
SPH2
X: 0.00 Y: 0.00 Z: 0.00
Vx: 0.00 Vy: 0.00 Vz: 0.00
Nx: -0.97 Ny: -0.26 Nz: 0.00
Fuel Remaining: 100%
10x

Enforcing security



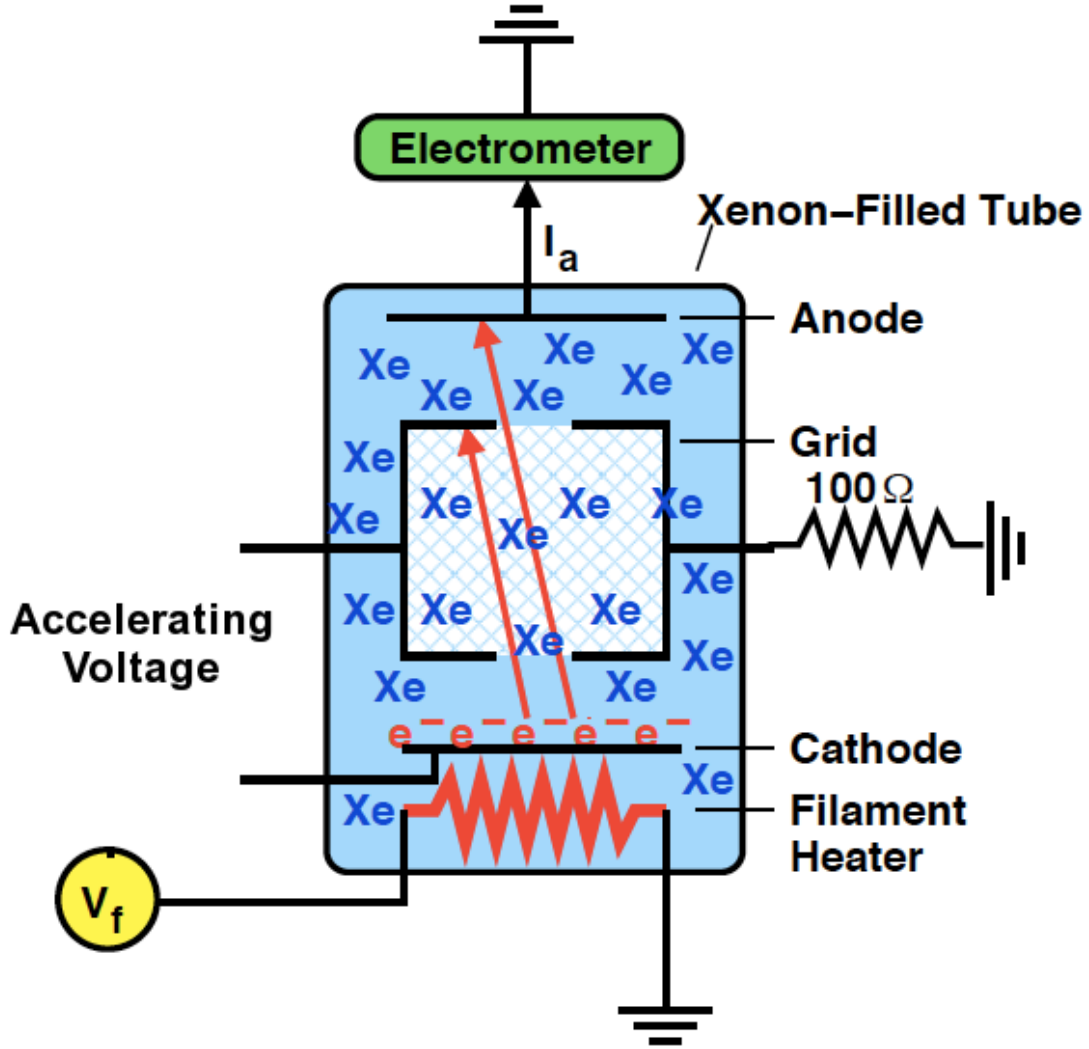
Background: bismuth

- White/silverish, crystalline, brittle, very dense, highly diamagnetic metallic element
- Very sensitive to high temperatures
- Very viscous and cools rapidly
- Pretty colors and cool shapes



1. http://www.facts-about.org.uk/science-element-bismuth.htm
2. http://upload.wikimedia.org/wikipedia/commons/6/65/Bismuth_Crystal.jpg

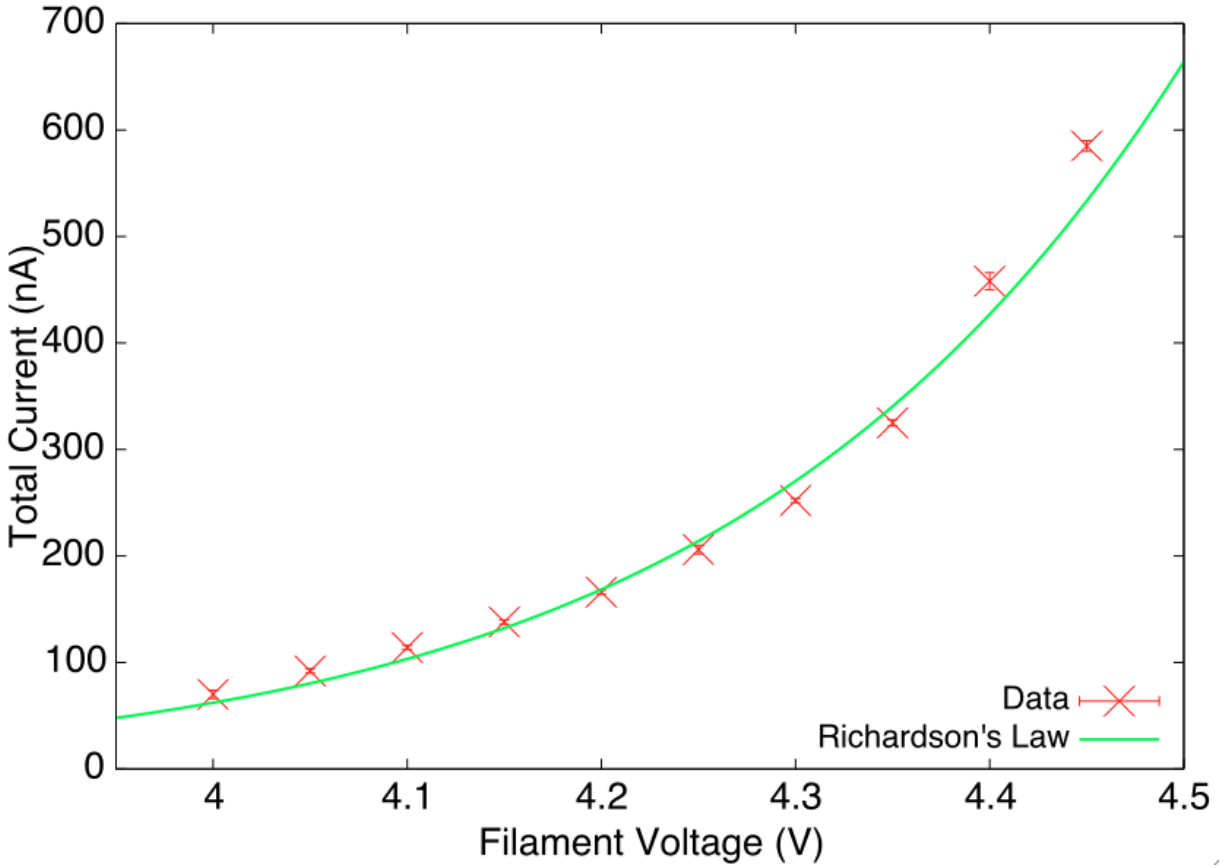
Apparatus



- Can freeze out Xe using liquid nitrogen

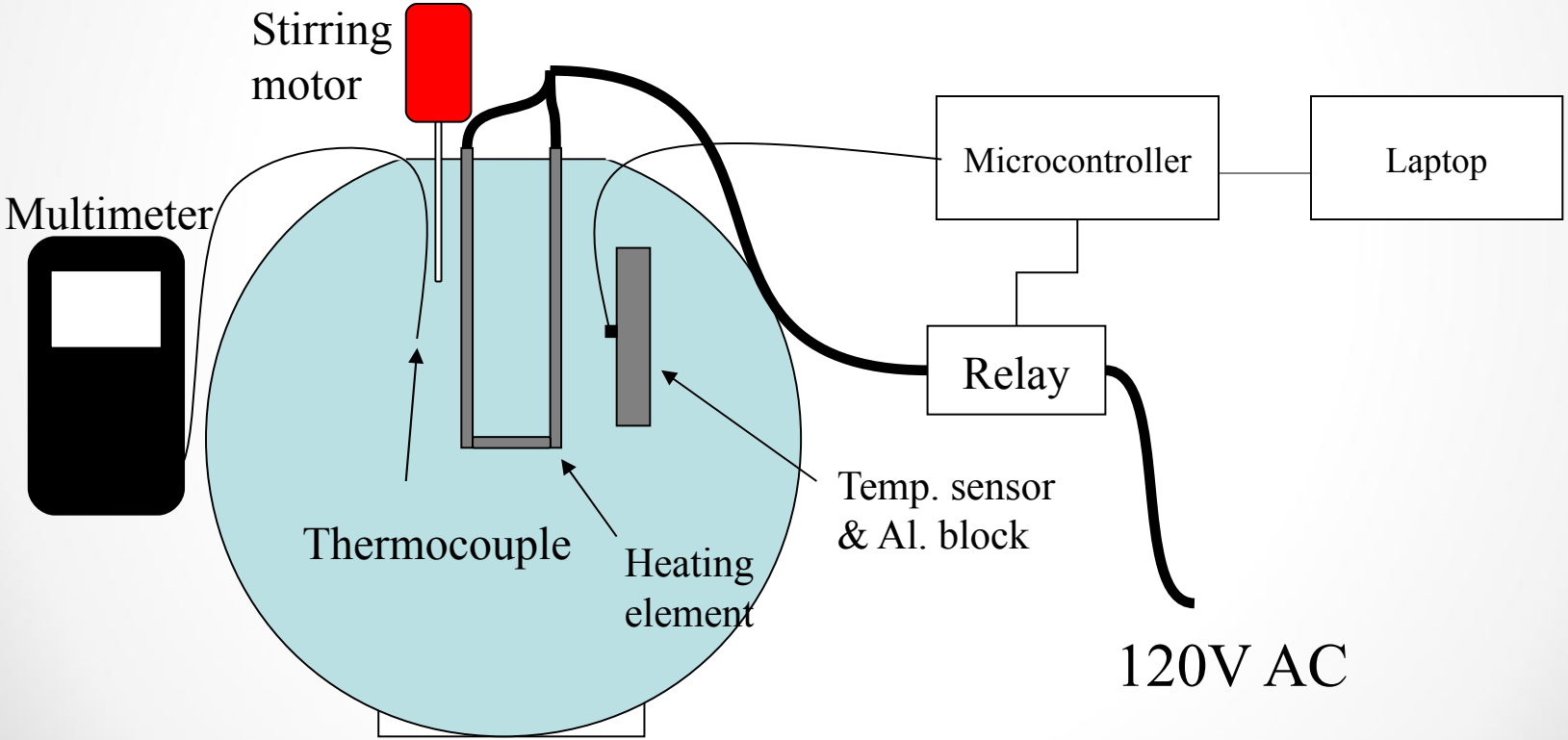
Richardson's Law

- $I \propto T^2 e^{\frac{-W}{kT}}$
- Only radiative heat transfer $\rightarrow V^2 \propto T^4$

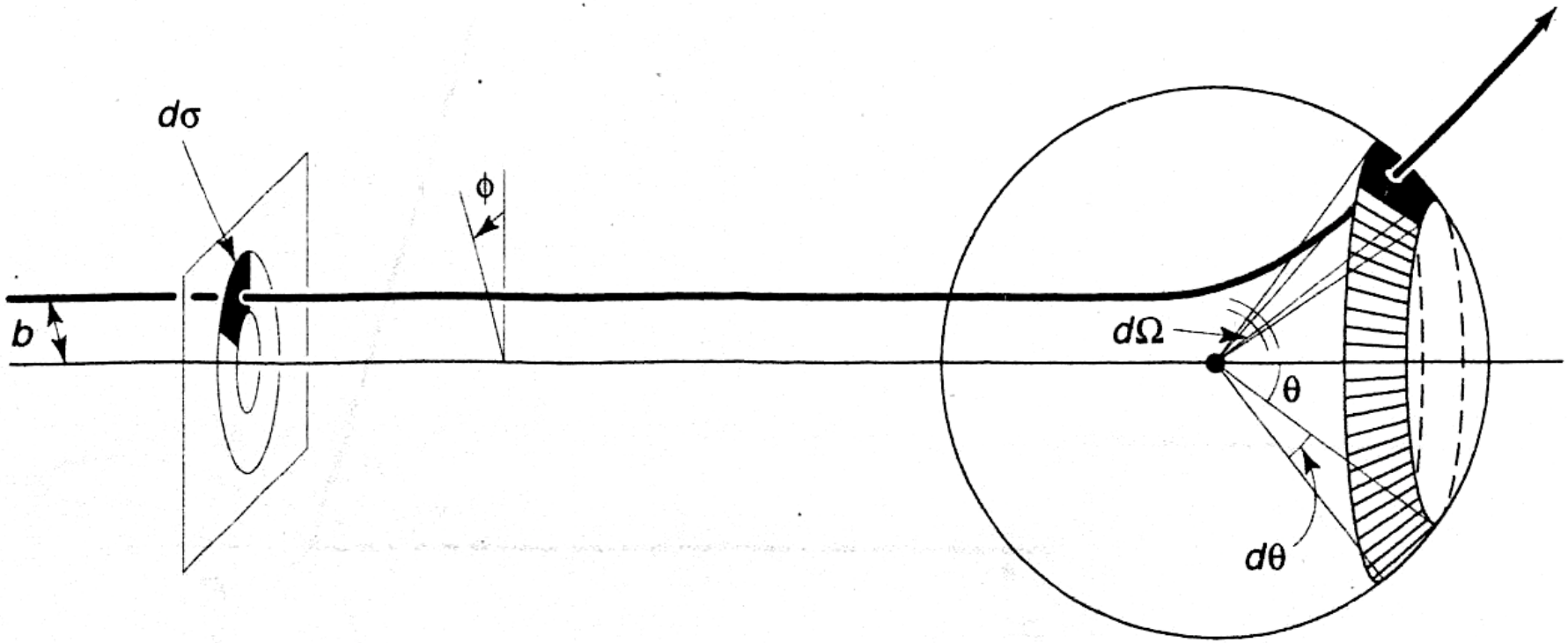


$$\chi_r^2 = 44.7$$

Temperature Regulation



Scattering



- $\mathrm{d}\sigma = D(\theta)\,\mathrm{d}\Omega$
- $\sigma(E) = \int D(\theta)\,\mathrm{d}\Omega$

CHALLENGE ACCEPTED

Sodium Acetate

Pattern avoidance

Let $\sigma \in S_n$, and $\phi \in S_k$ where $k \leq n$.

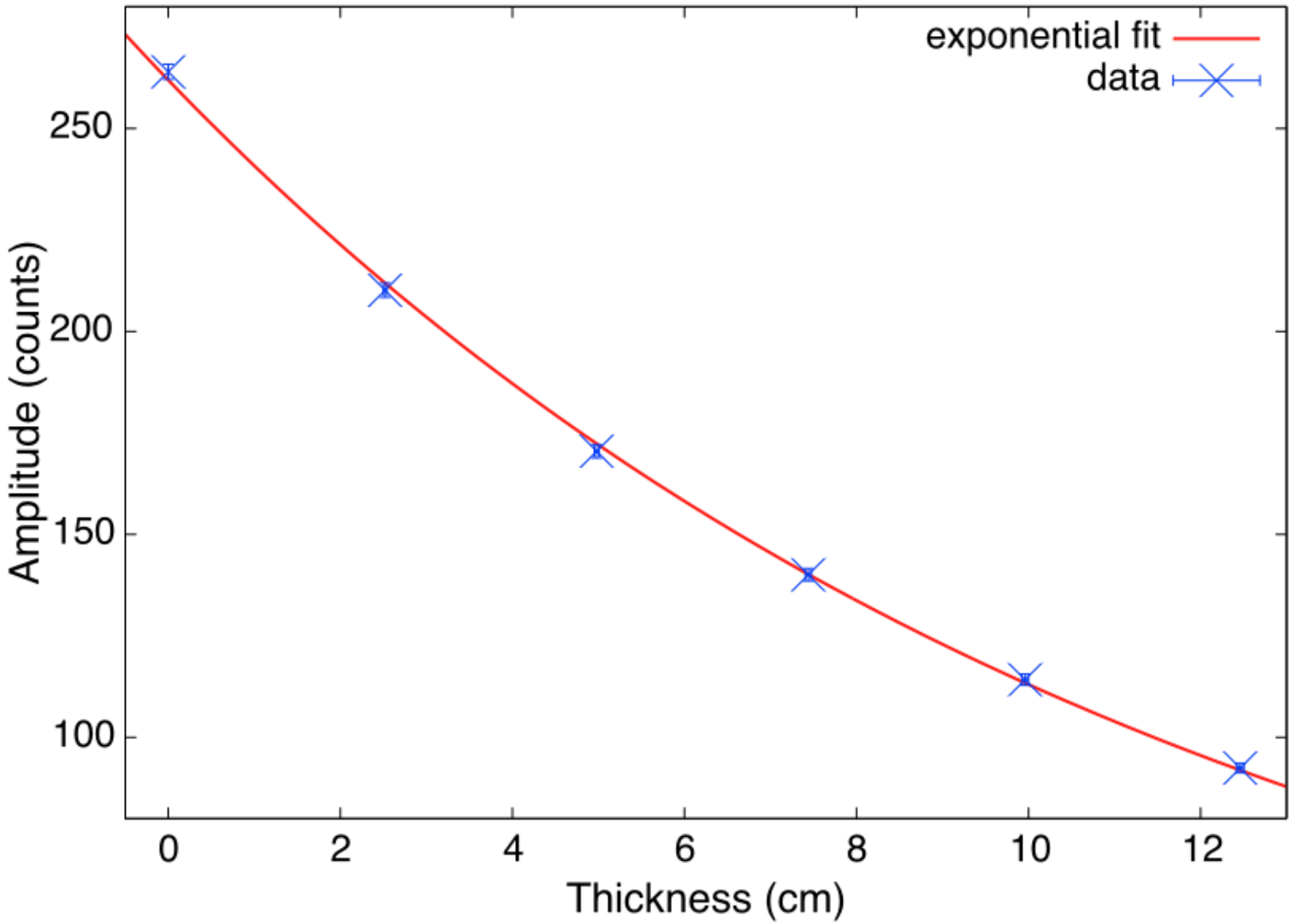
Definition

We say that σ contains ϕ if there exists a subsequence of σ which is order isomorphic to ϕ. Otherwise, we say that σ avoids ϕ.

General Structure

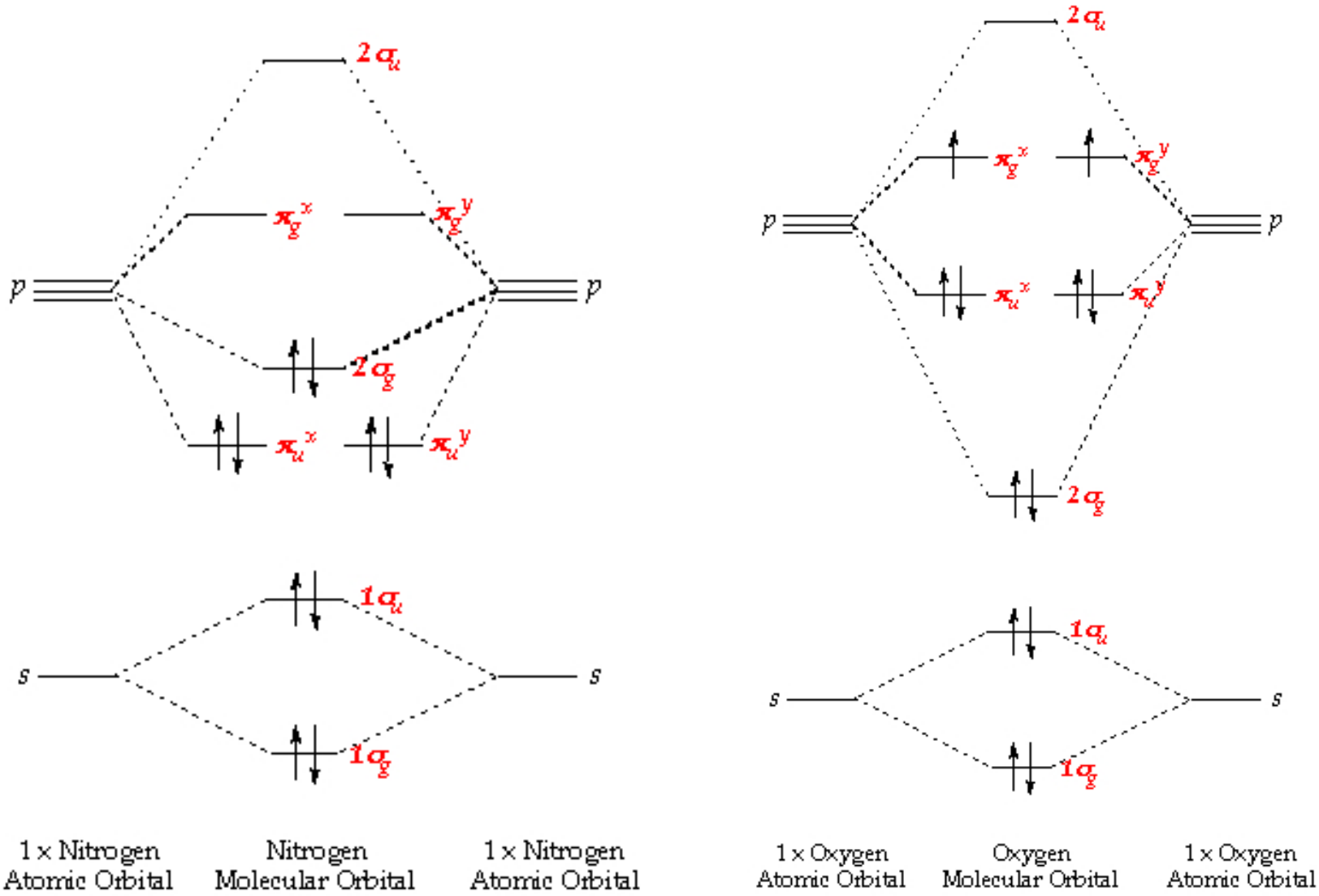
	Victor stands outside
Peggy: Prepare	
	Peggy vanishes into the cave
Peggy: Commit	
Victor: Challenge	
Peggy: Respond	

Attenuation

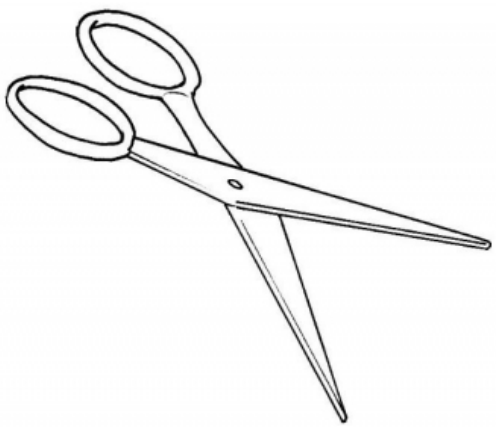


$$\chi_r^2 = 1.00$$

Paramagnetism: N_2 vs. O_2



Scissors



Ideas from the classification of cycle structure

First, note that if $x \leq c$, we have

$$\sigma_{abc}(x) = x + a + b.$$

For ease of notation, let $d = c - a$. If $c < x \leq b + c$, we have

$$\sigma_{abc}(x) = x - d,$$

and if $x > b + c$, we have

$$\sigma_{abc}(x) = x - a - b.$$

Zero-Knowledge Proofs

Showing you *can* do something, without showing how

Alex Dehnert

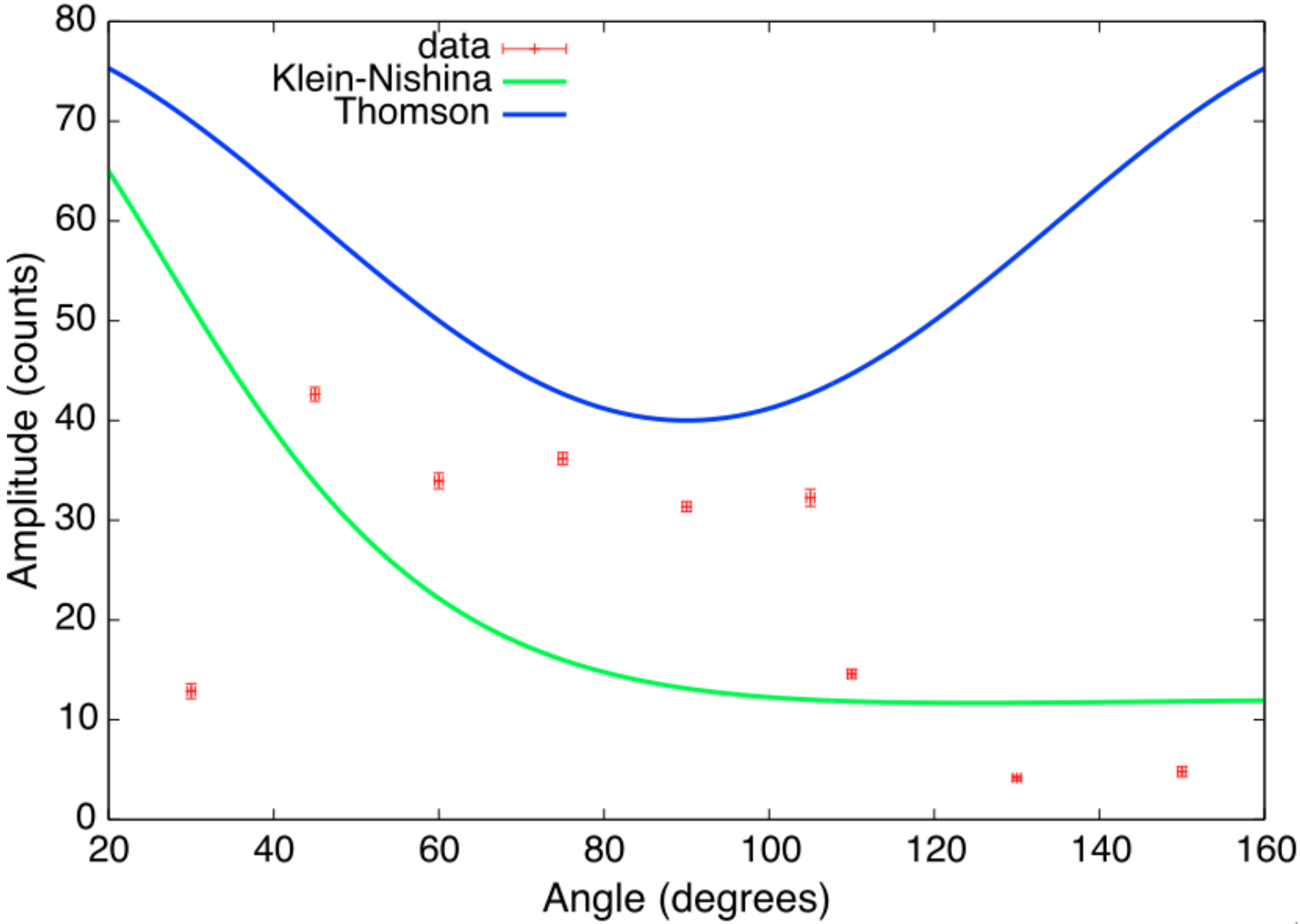
6.UAT

Fall 2011

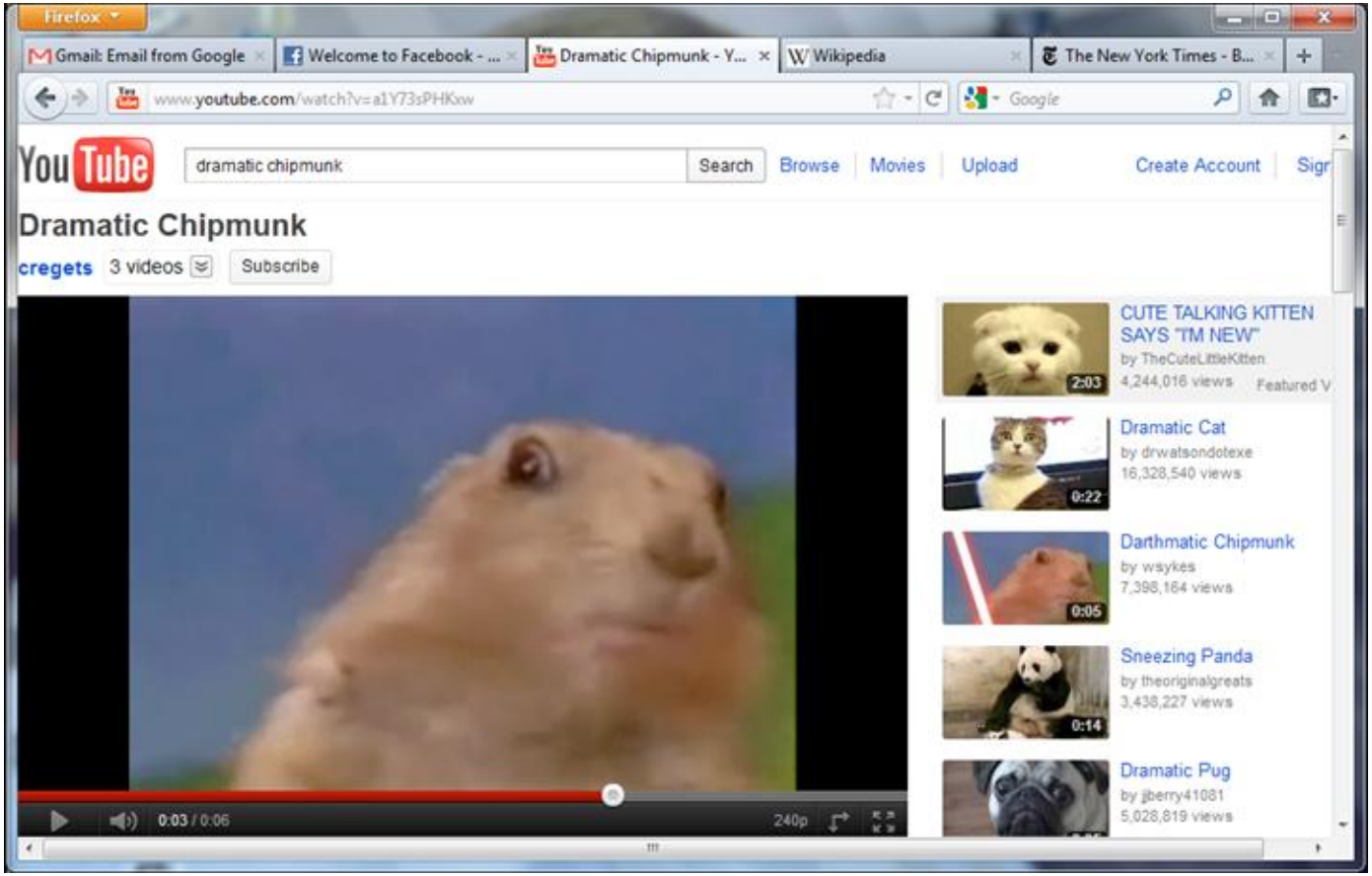
What's new?

- Intrusion detection based on syscalls *isn't* — plenty of people have done that
- However, generally, that's vulnerable to attacks against the agent
- So, develop a version that gathers data using vprobes

Amplitudes

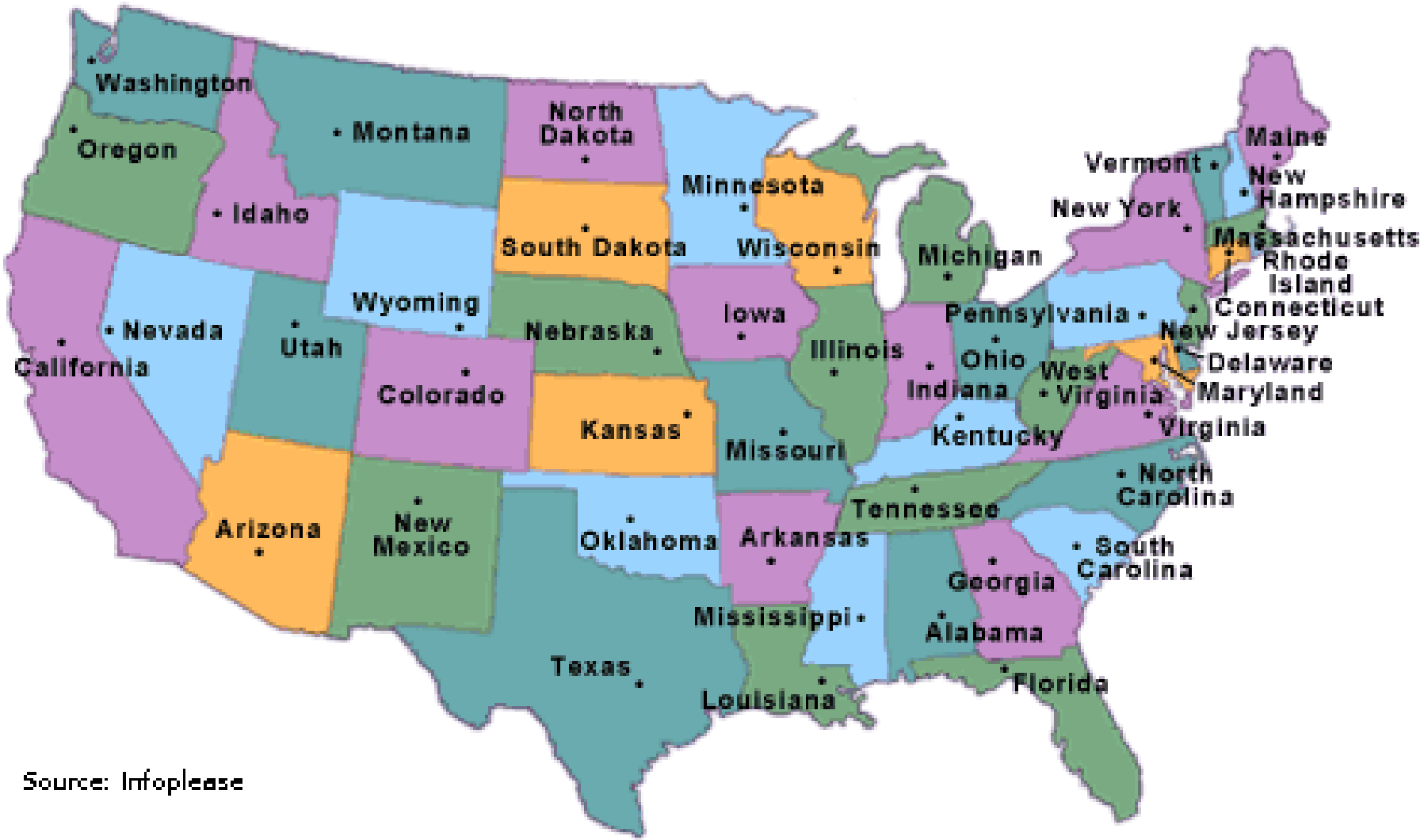

data
Klein-Nishina
Thomson
Amplitude (counts)
Angle (degrees)
0
10
20
30
40
50
60
70
80
20
40
60
80
100
120
140
160

What if a webpage crashes?



Map 3-coloring

Given a map, prove that it can be colored using only three colors (and that you know a coloring).



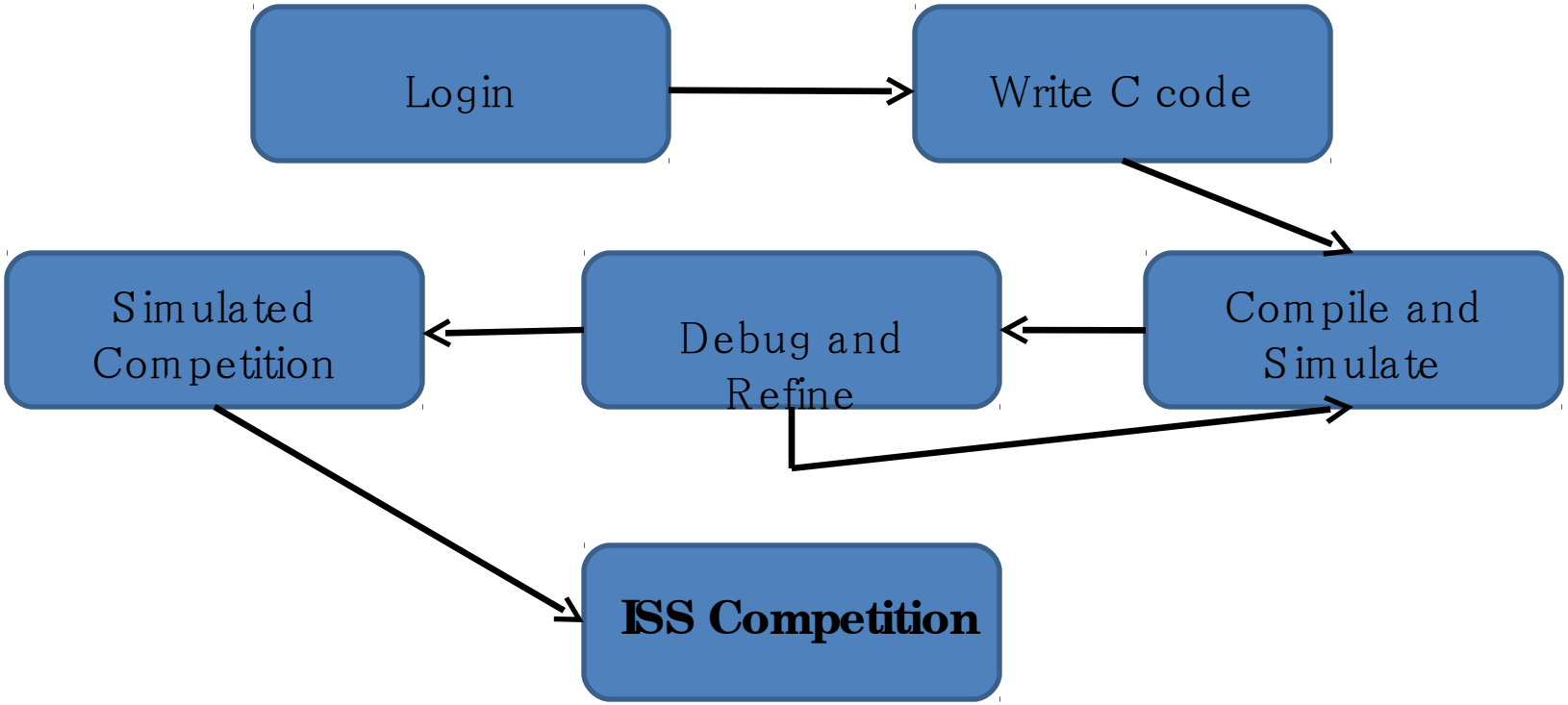
Intrusion Detection in Virtual Machines

Alex Dehnert

VI-A – VMware

Fall 2011

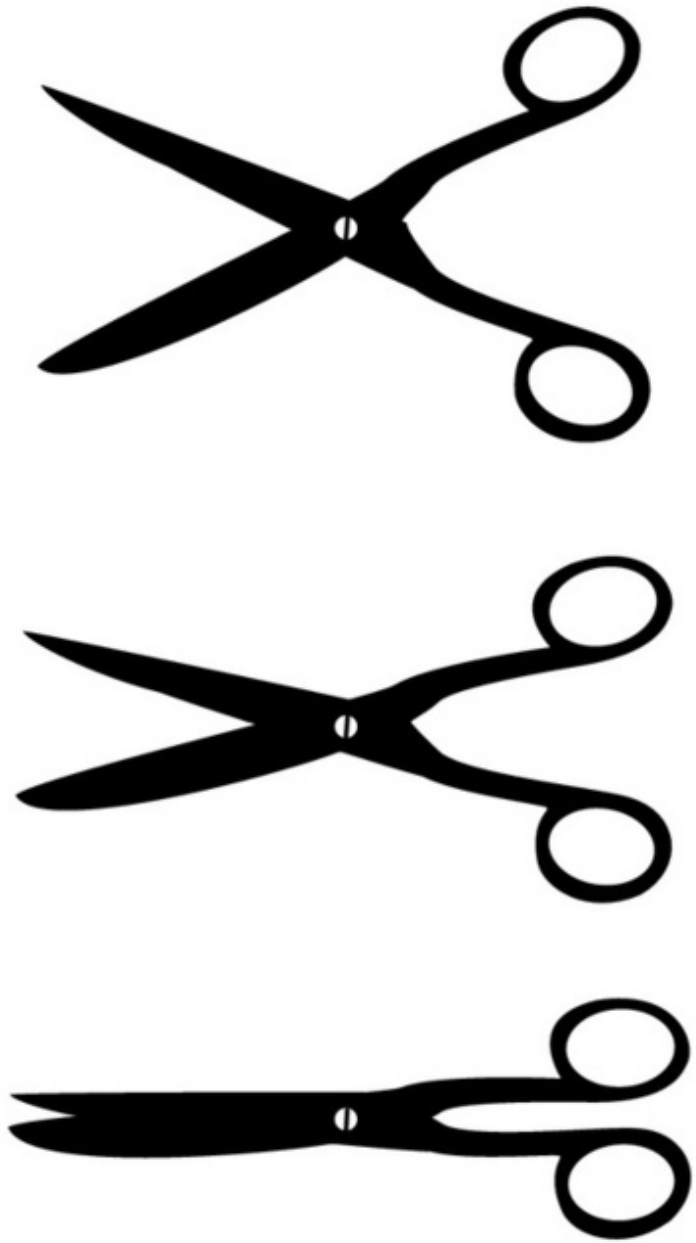
The SPHERES Process



Proof of classification of *abc*-permutations

Assume that σ is reverse layered and avoids 4321. Then it has at most three layers, so it is an *abc*-permutation.

Edward's Gambit (SSS)

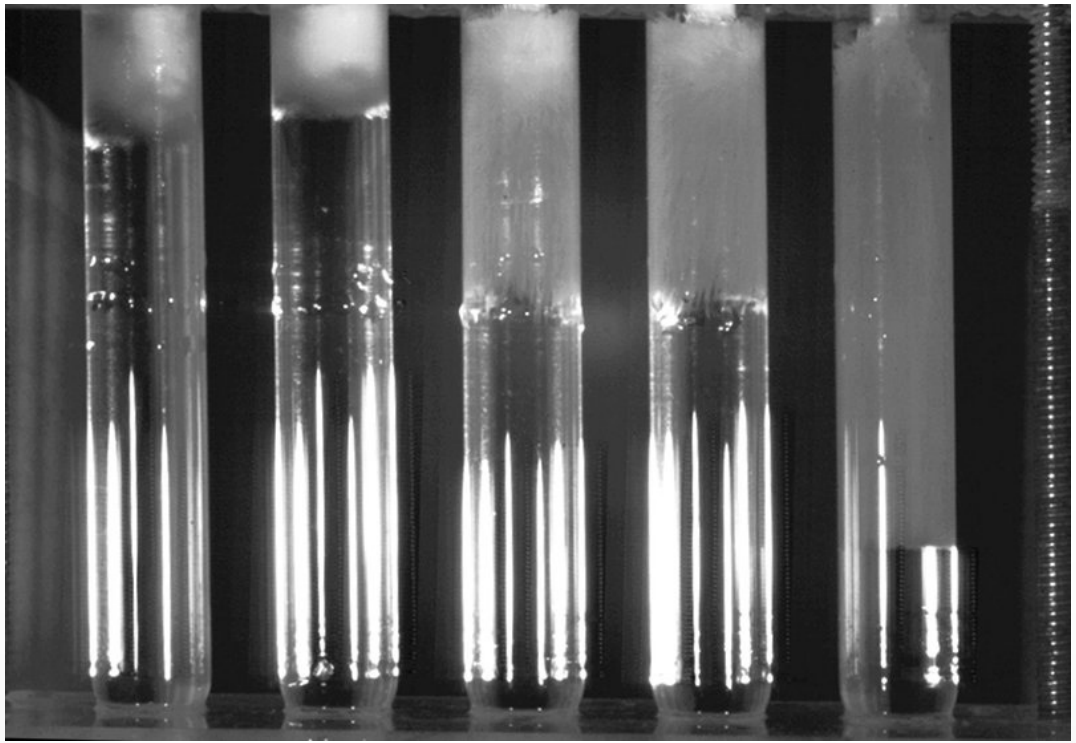


Observation of the Photoelectric Effect

Daniel J. Fremont

Massachusetts Institute of Technology

High Speed Crystallization of Sodium Acetate



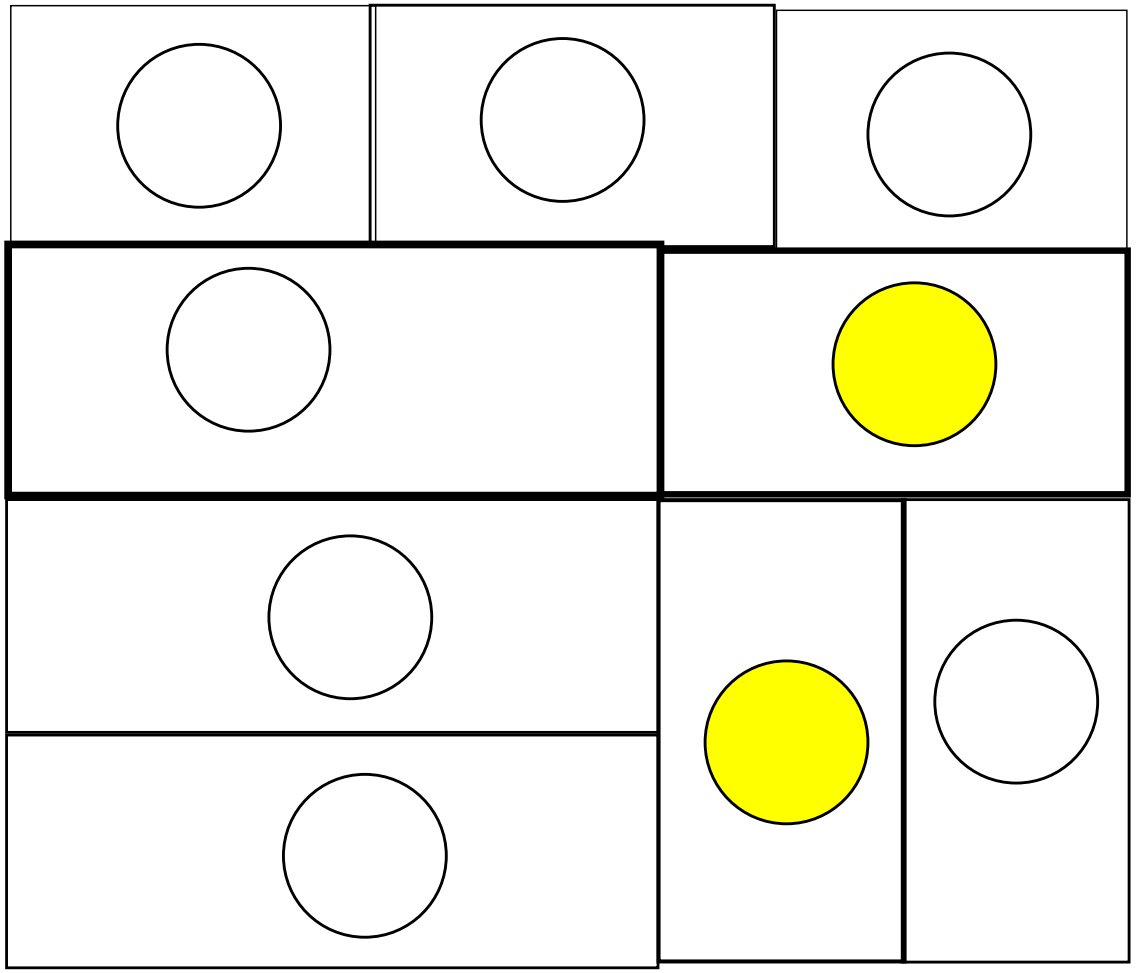
Robin Deits, **Sally Wolfe**, Daniel Ron, Bayo Olatunji

Improvements and Extensions

- More stable probe setup to allow more accurate determinations of field strength
- Greater sensitivity to allow use of higher concentrations
- Removing dissolved oxygen

Map coloring ZKP

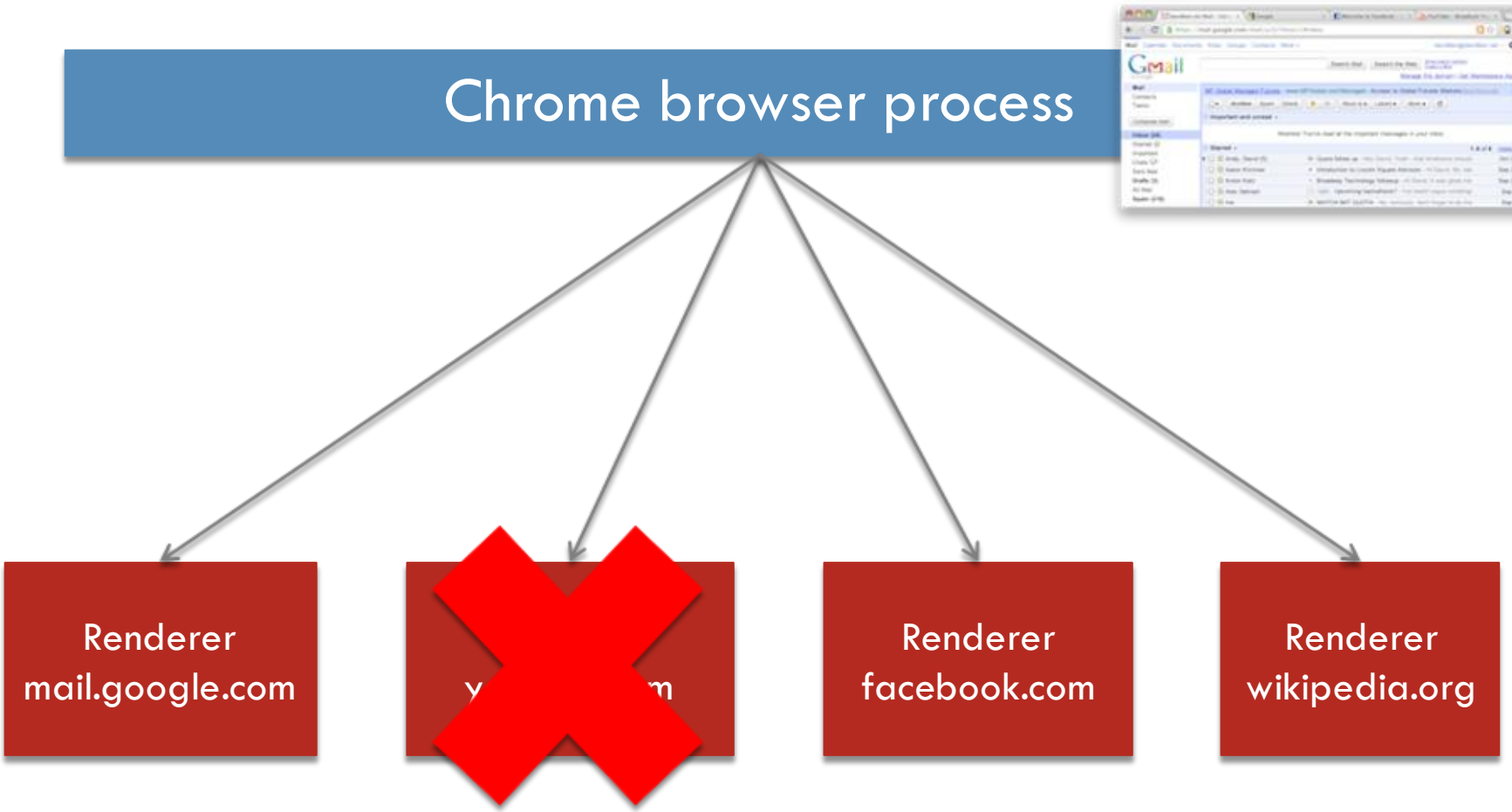
Challenge



Matter Waves and Interference

- Electrons and atoms cannot be treated as billiard balls
- Objects are diffuse, described by a wave function
- Interference between wave functions can produce unexpected effects
- Ramsauer-Townsend: $\sigma = 0$ for a particular energy

Multi-process browsing



Why bother?

- Crashes mean browser bugs
- Why not just write correct code?

5,000,000

Principle of least privilege

Each component of your system should have only the rights it needs and no more

- Limit damage when things go wrong
- Fewest privileges to parts most likely to fail

Avenues for further research

1. What is the cycle structure of layered permutations?
2. What is the structure and number of permutations which avoid 132, 213, and another permutation of length at least four?

Einstein's theory

- Planck's quantized oscillators
- Photons, with $E = h\nu$
- Intensity $\equiv$ number of photons
- One photon, one electron

$\Downarrow$

- Energy of emitted electrons independent of intensity
- Energy dependent on frequency
- Minimum cutoff frequency

Rock Paper Scissors:

Real Professional Strategy

Nathan Benjamin & Xavier Jackson
(nathanb@mit.edu, jaxxson@mit.edu)

Results

Close up of solidified bismuth. Color variation from crystal formation is visible. Size is roughly ~3 mm across. f/16, 90mm lens

Nuclear Magnetic Resonance: Effect of Paramagnetic Ions on Relaxation Times

Daniel J. Fremont

8.13 — Junior Lab
Massachusetts Institute of Technology

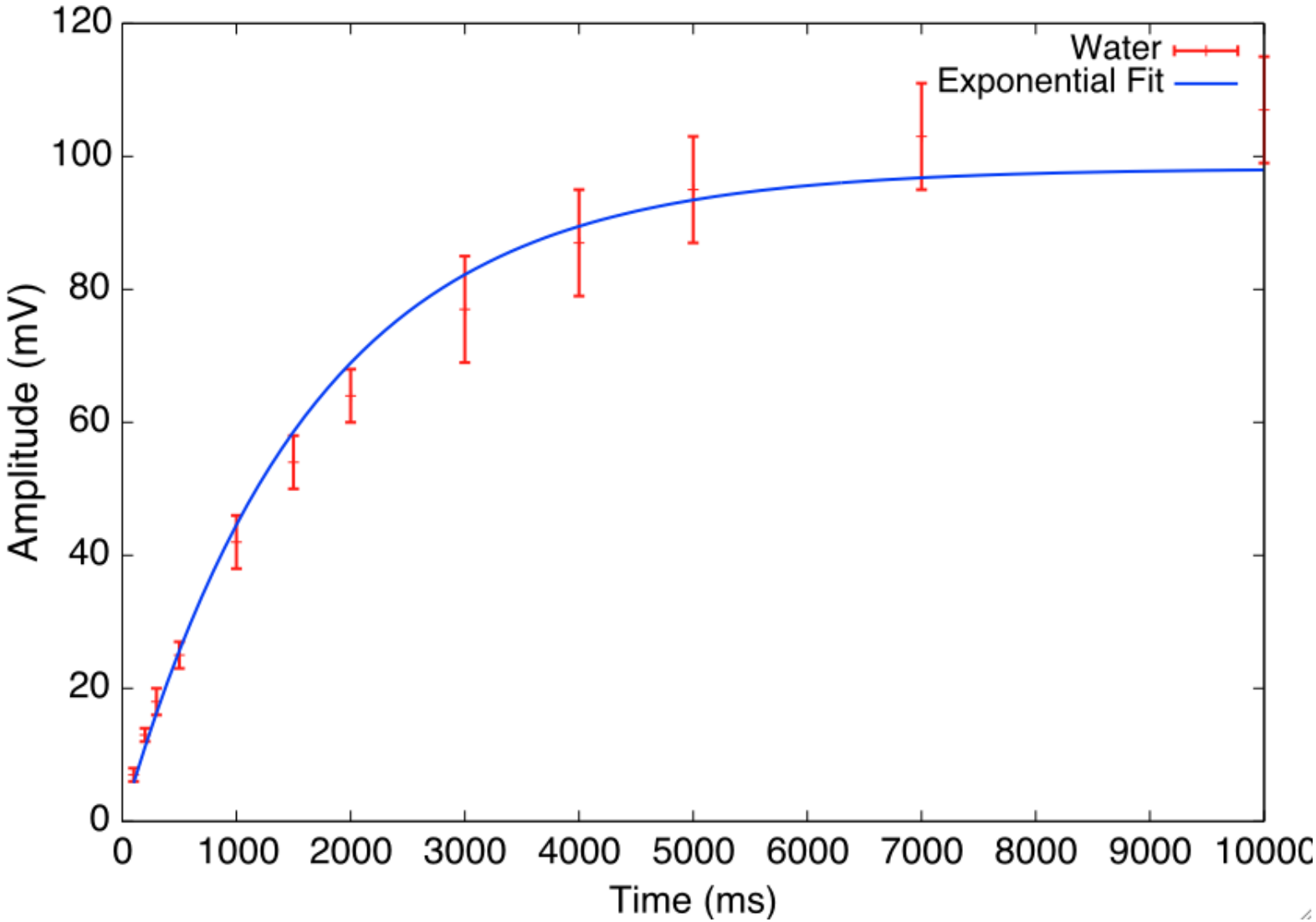
Definition of $\mathbf{p}_k(n)$

Since

$$\mathbf{p}(n) = 1 - \sum_{s=2}^{n} \mu(s) f(n, s),$$

we have

T1 Measurement



$$T1 = (2108 \pm 240)ms \qquad \chi_r^2 = 1.13$$

Avenues for further research

1. What is the cycle structure of layered permutations?

Results

- Proton magnetic moment: $(1.424 \pm 0.083) \cdot 10^{-26}$ J/T
  - Accepted value: $1.411 \cdot 10^{-26}$ J/T
- $\frac{1}{T1}$ grows linearly with Fe^{3+} concentration
- $\frac{1}{T2}$ grows faster than linearly with Fe^{3+} concentration

Results

- Minimum σ occurs at $0.53 \pm 0.077\ V$
  - Significantly off from true value of 0.9 V
- Random errors insufficient
- Systematic errors
  - Contact potential
  - Nonzero initial electron energy
  - Unequal filament temperatures
- Corrected value: $0.88 \pm 0.092\ V$

Reverse layered permutations

Definition

A permutation ϕ is called reverse layered if it is of the form $q_1 q_2 \dots q_k$, where the q_i are strings of consecutively increasing numbers and $q_i > q_j$ if $i < j$.

abc-permutations

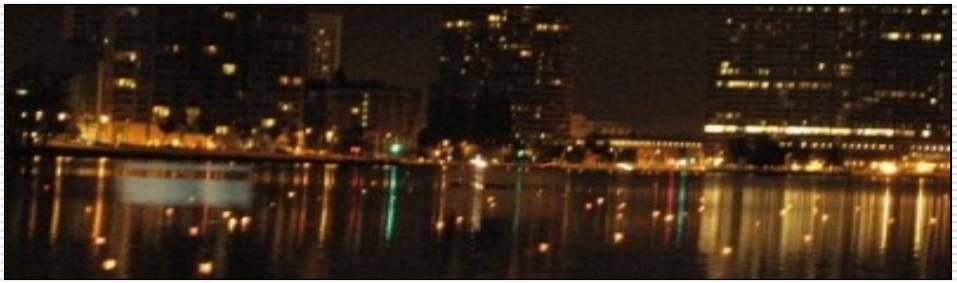
Definition

Let *abc*-permutations be elements of S_n obtained by partitioning $[n]$ into three blocks of length a, b, c and exchanging the first and last blocks.

Examples

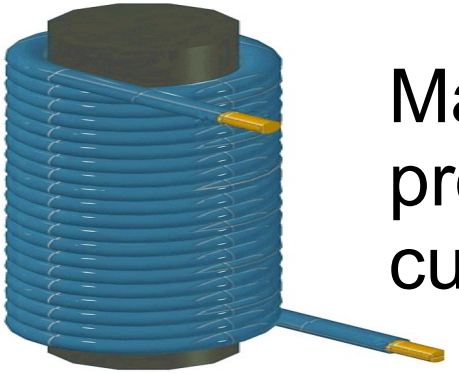
[67851234]
[67812345]

Sample Tasks



What would you learn if you walked through LA wearing 30 pounds of carrots, led a squirrel fishing party, challenged a dragon, asked for help inflating a large duck, and solicited strangers for a dinner invitation?

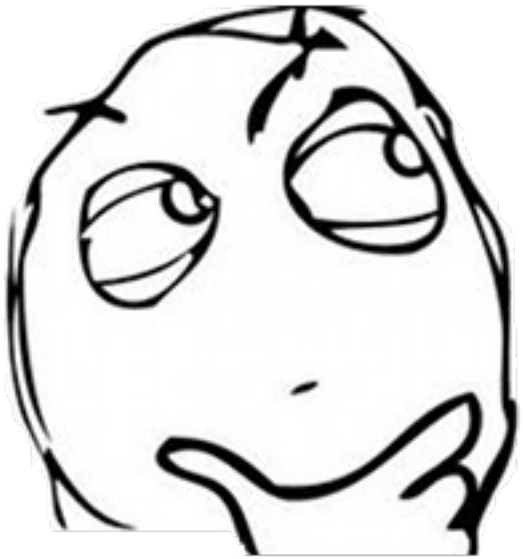
Levitation!



Magnetic field proportional to current

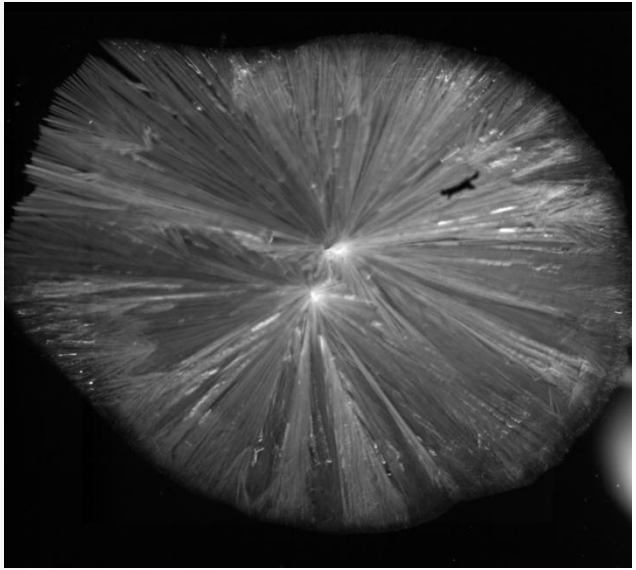
Position sensor

- Character
- Plot
- Conflict
- Structure
- Setting
- Theme
- Motif
- Style
- Imagery
- Symbolism
- Dialogue
- Perspective

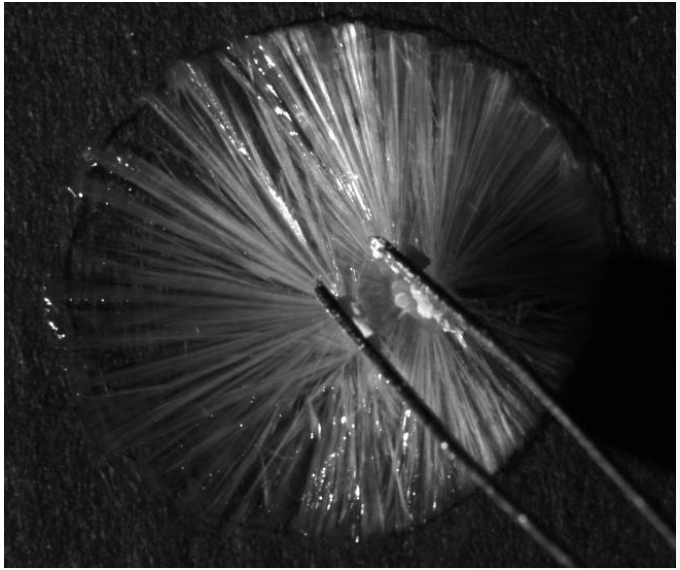


Procedure: boiling setup

Results

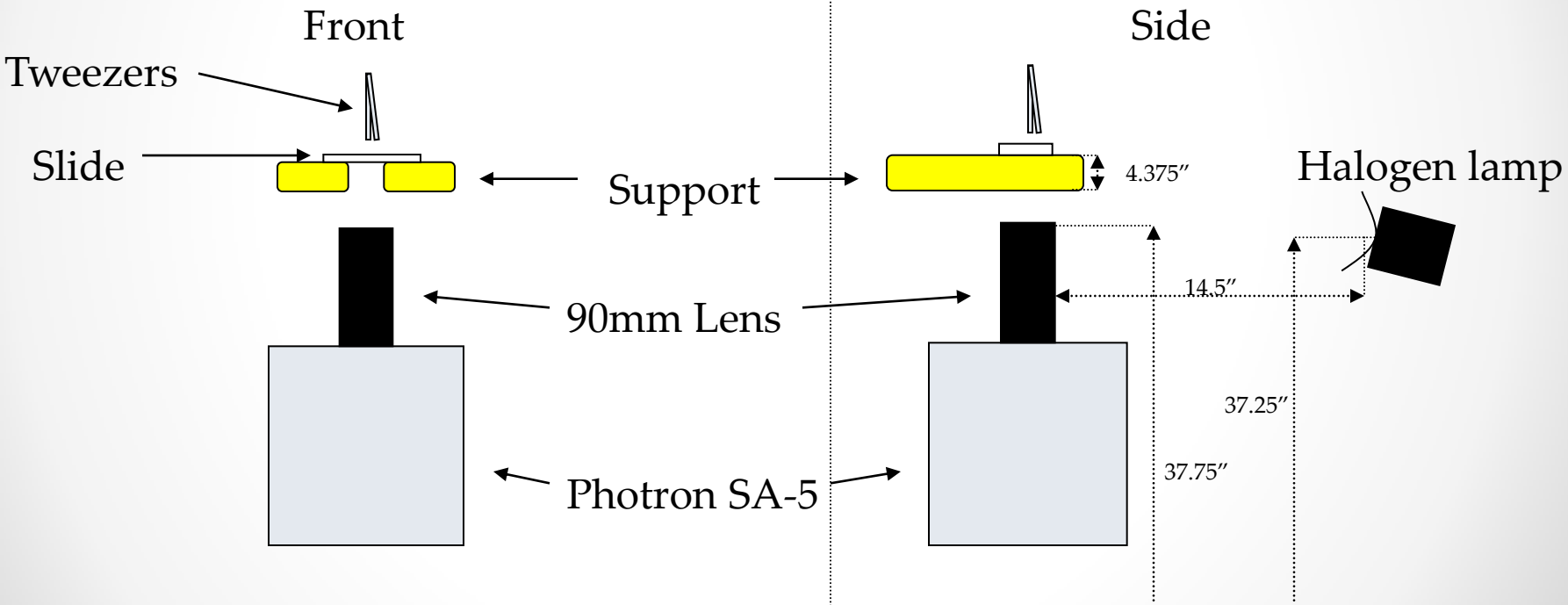


Crystallization of supersaturated Sodium Acetate solution from below. Three drops from an eyedropper. Two points of emanation. Shot at 1000 fps, f/8 90mm lens.



Crystallization of supersaturated Sodium Acetate solution from above. Crystals appear to be on top of the solution. Three drops from an eyedropper. Two points of emanation. Shot at 1000 fps, f/11, 90mm lens. Brightness increased 30% for clarity.

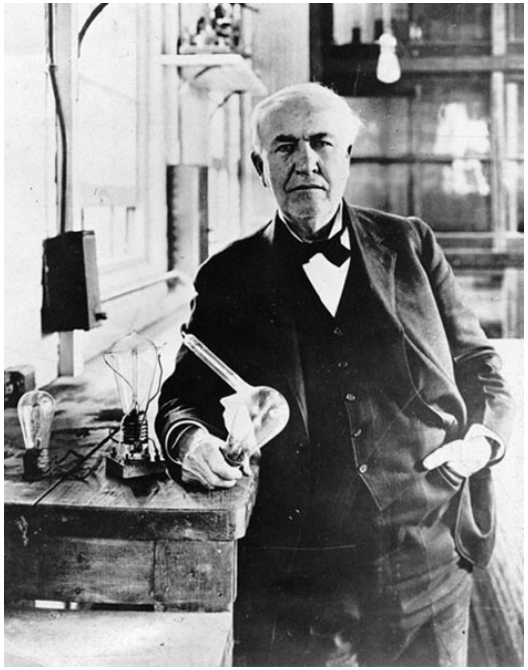
Procedure: underneath setup



Distributed Innovation

There are a lot more smart people than geniuses

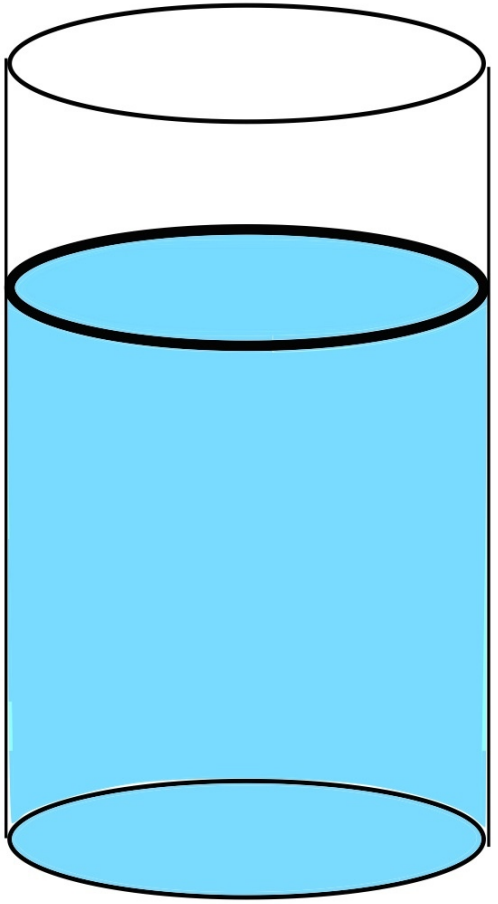
1 in a million?



Millions and billions.

New technologies enable collective genius

Filling a glass to a specific height

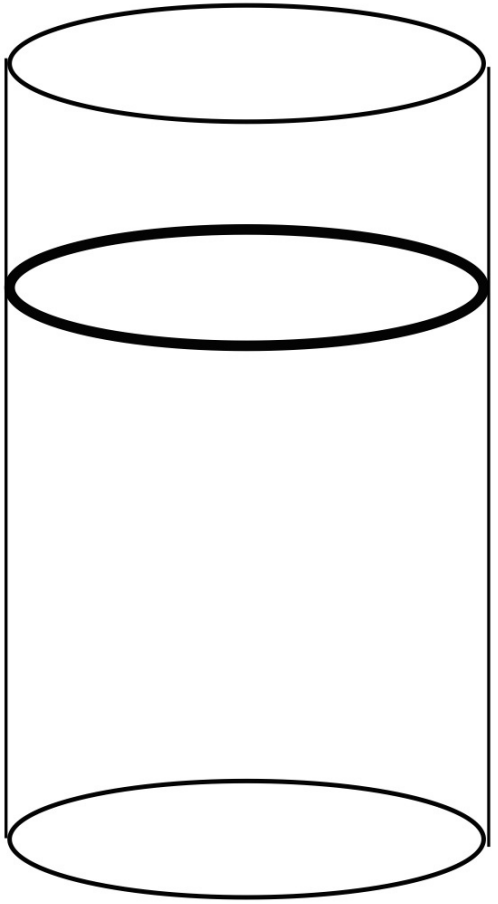


Constant rate of flow

Time = volume/rate of flow

- Words

Filling a glass to a specific height



Playing in the sandbox

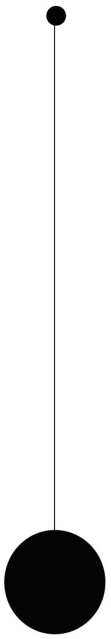
- How tab isolation works
- Sandboxing
- Principle of least privilege

Goals:

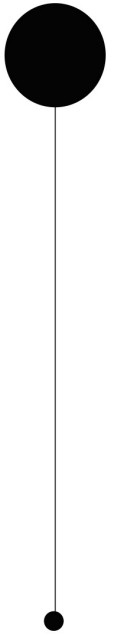
- Observe crystallization process
  - Targets: Sodium Acetate, Bismuth
- Make measurements of speed and process of crystallization
- Determine feasibility of future quantitative studies

Equilibria

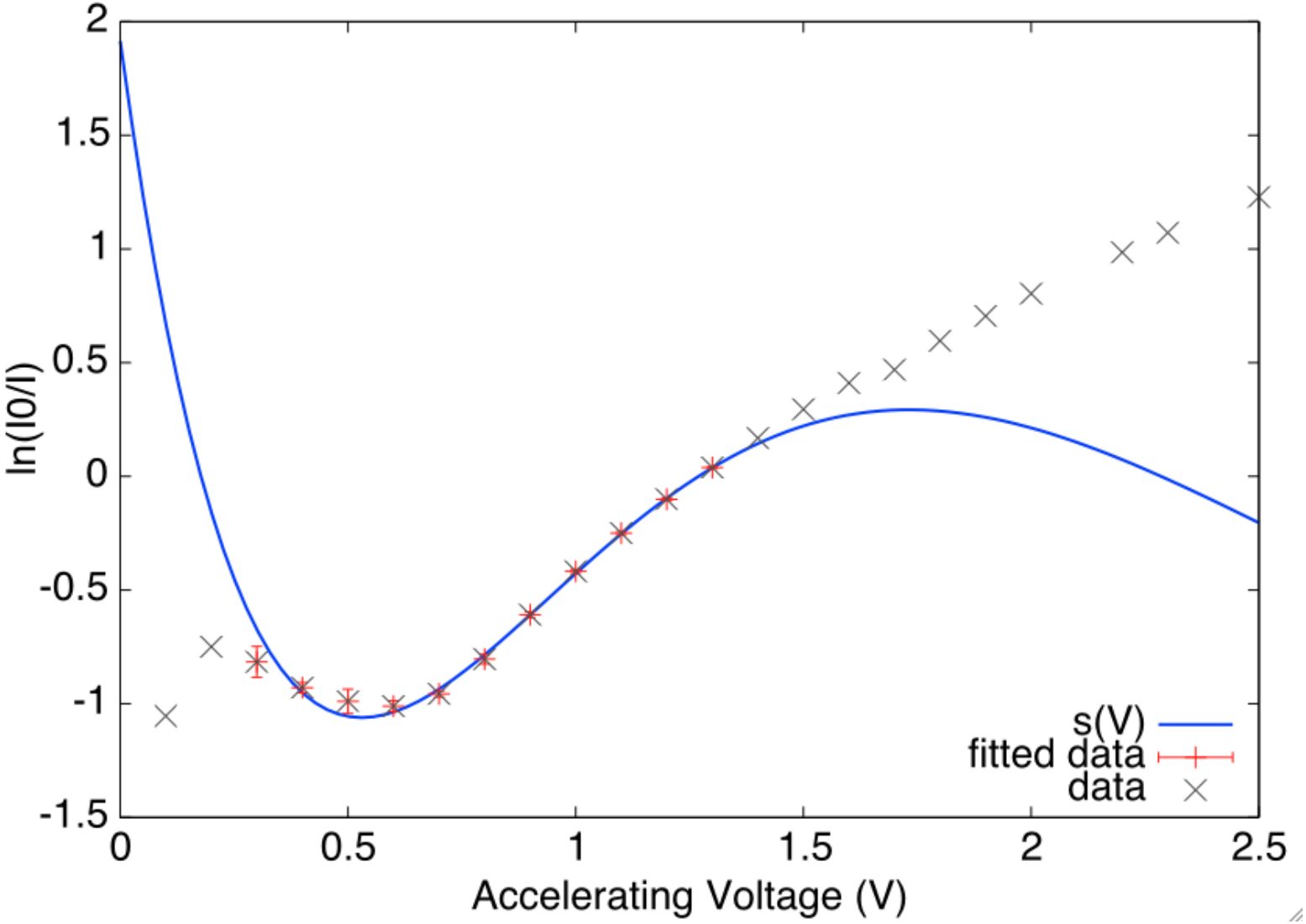
Stable



Unstable

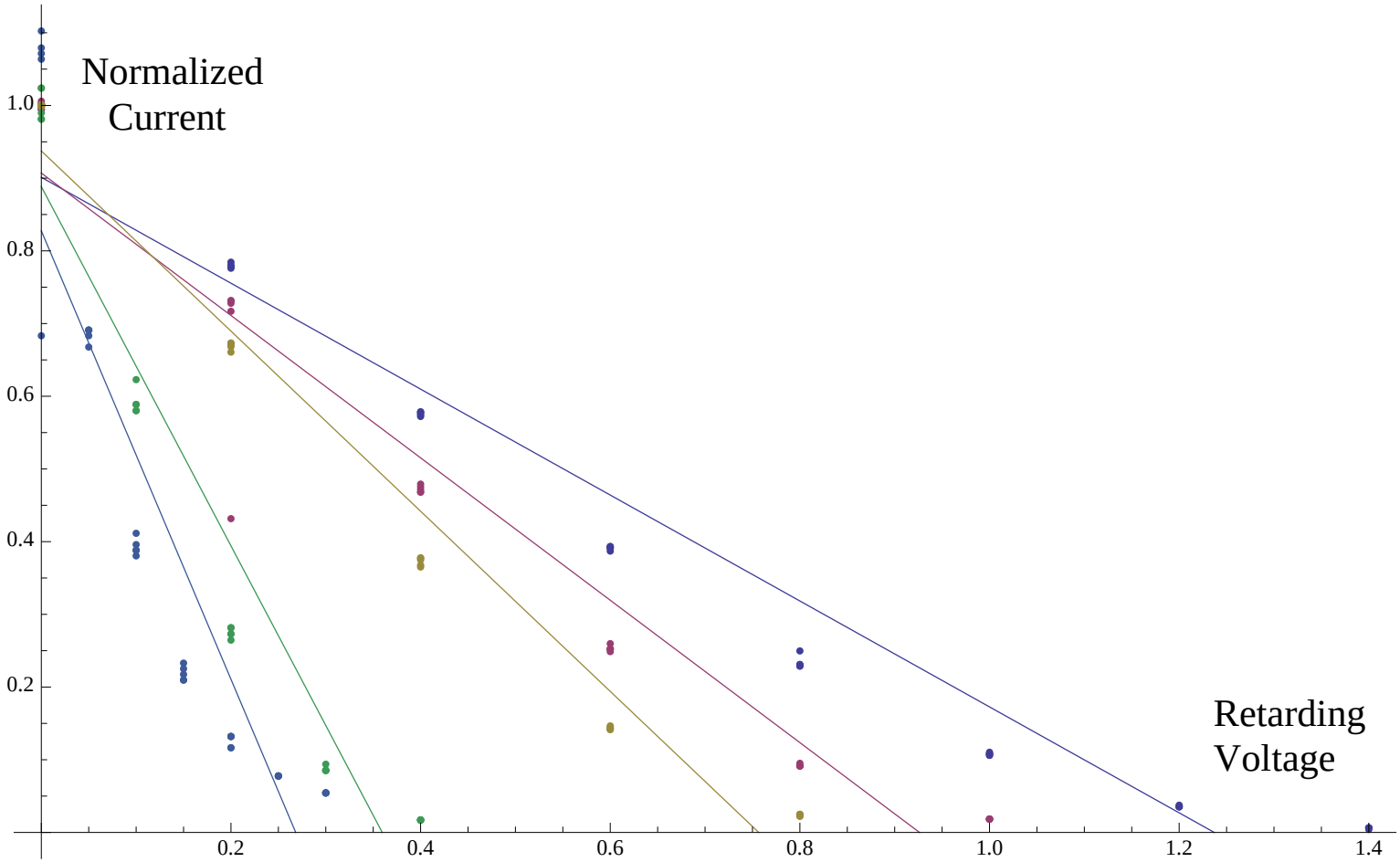


Cross-Section Measurements



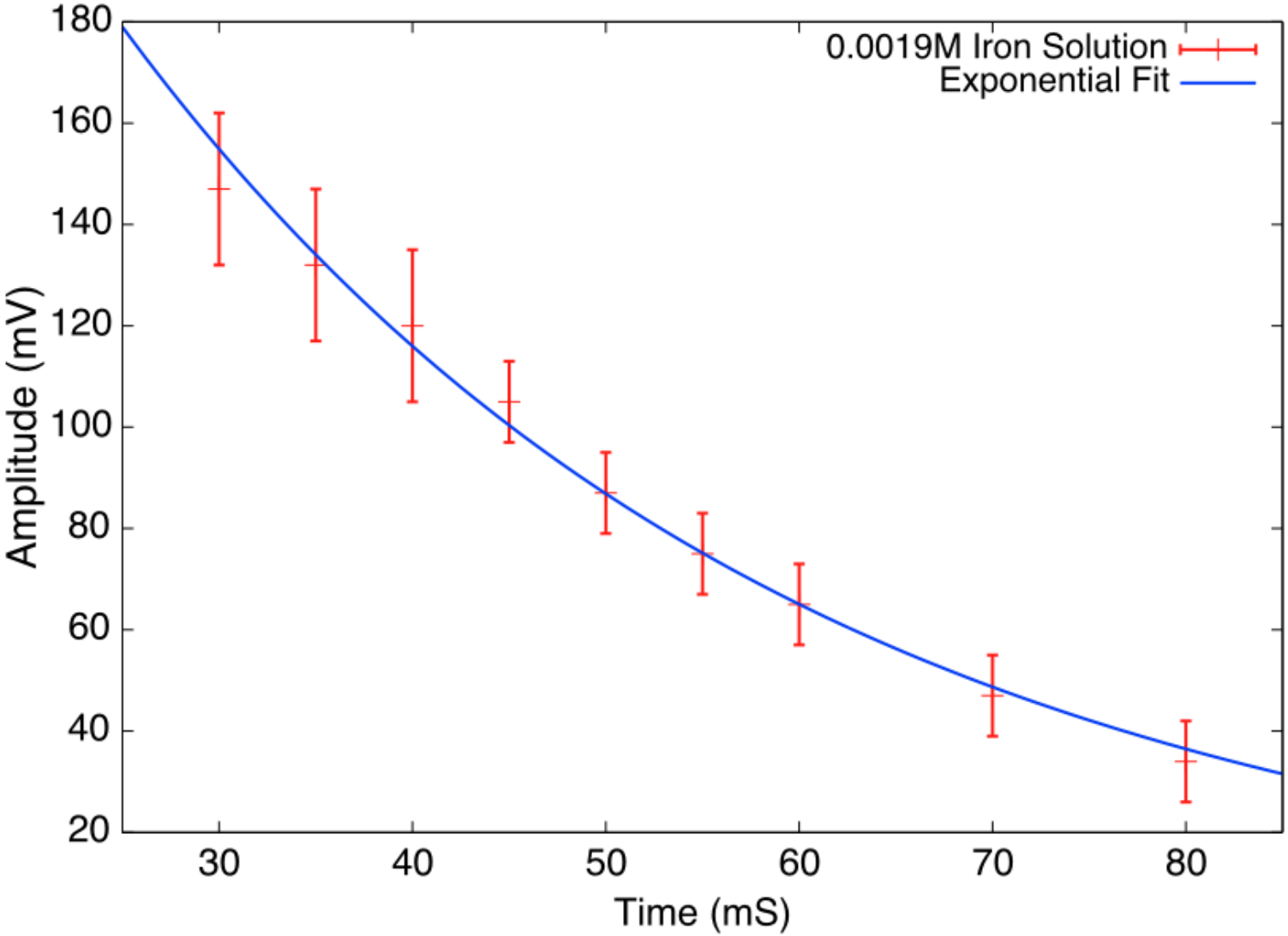
$$\chi_r^2 = 1.93$$

Current vs. Retarding Voltage



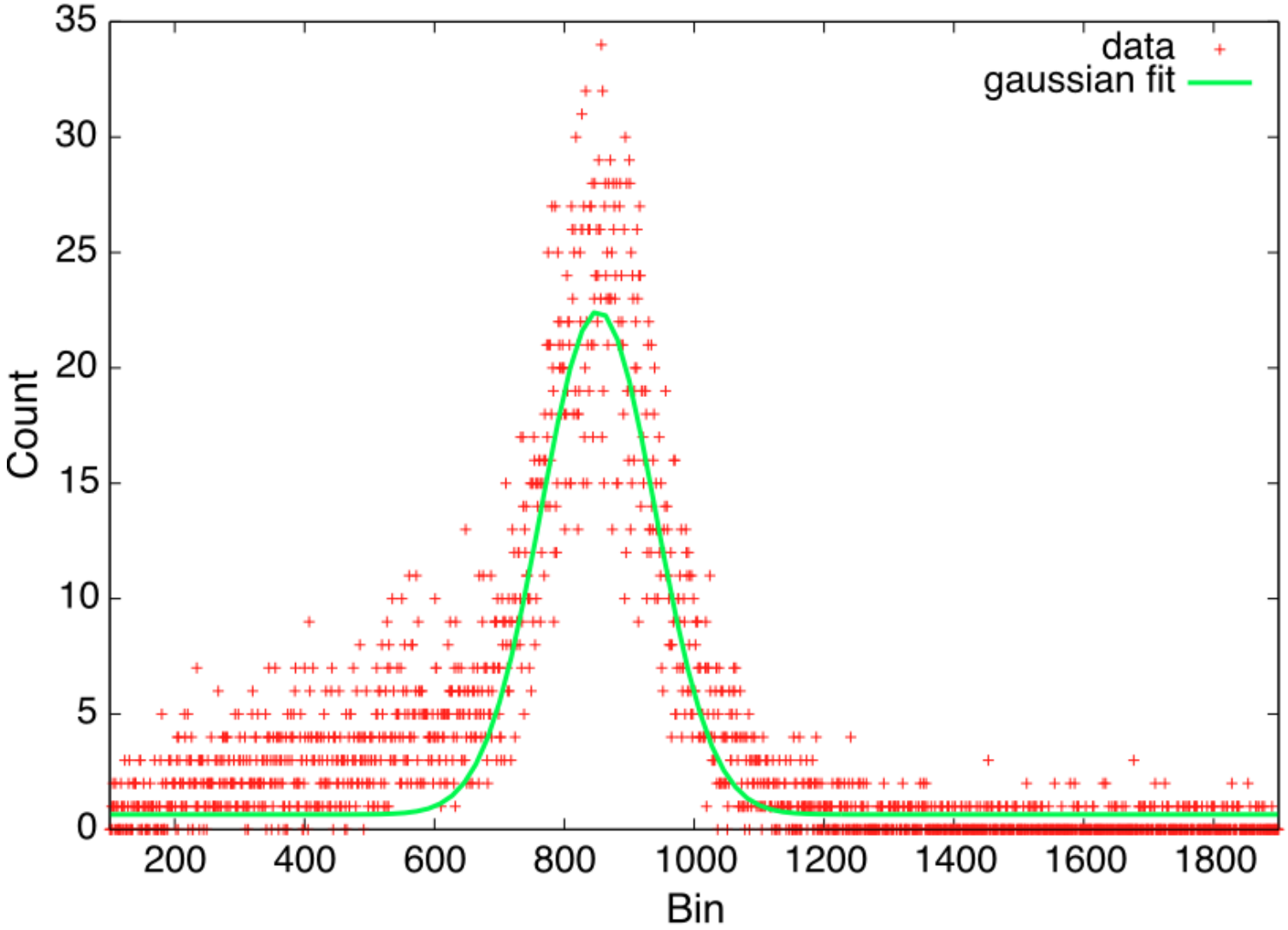
- Some expected features, with some extras
- Theoretical model?

T2 Measurement



$$T2 = (8.86 \pm 0.16) ms \qquad \chi_r^2 = 0.13$$

Data



$$\chi_r^2 = 0.95$$

Pattern avoidance and *abc*-permutations

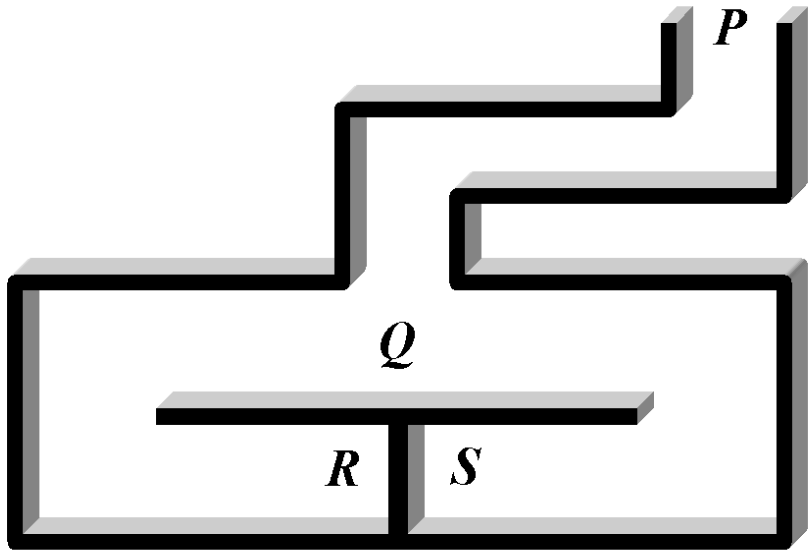
Theorem

The set of abc-permutations is the set of permutations which avoid 132, 213, *and* 4321.

In order to prove this theorem we make use of the fact that *abc*-permutations are *reverse layered permutations* with three or fewer layers.

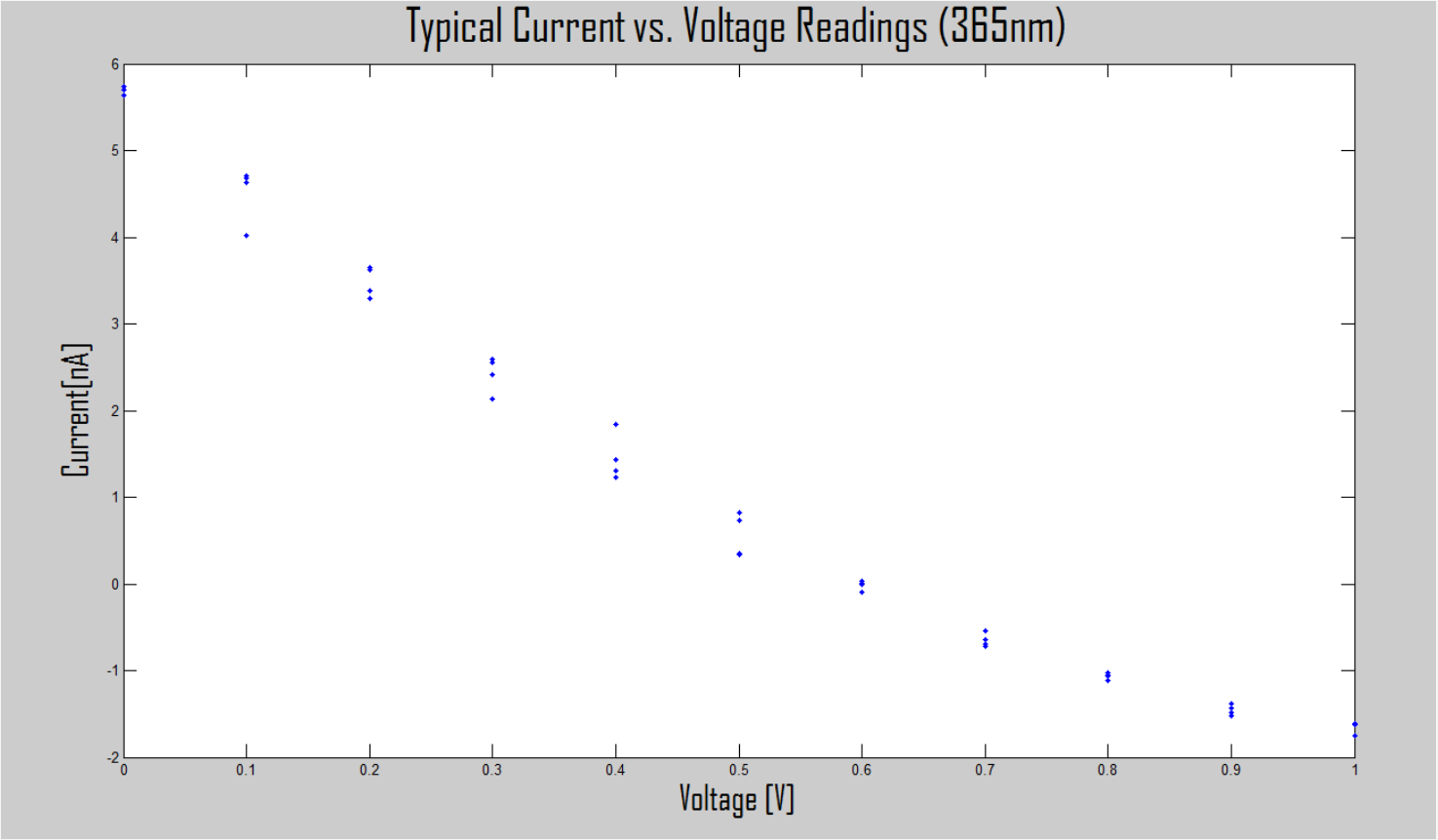
What if Peggy cheats?

- Victor stands outside at P
- Peggy picks R or S to hide at
- Victor comes back in, stands at Q, and calls out which side Peggy should return by
- If Peggy picked the correct side, she tricks Victor; otherwise, she has to admit she lied
- If Victor does this enough times, Peggy will guess wrong (one trial, 50% she succeeds; two trials, 25%; etc.)



Raw Data–Voltage vs. Current

275 Current, Voltage pairs collected over 5 different wavelengths



What comes after what?

Professor…

- McGonagall 28.5%
- Trelawney 8.9%
- Umbridge 8.7%
- Dumbledore 5.9%
- Lupin 5.8%
- Snape 4.6%
- Flitwick 3.9%
- Sprout 3.3%

from …

- the 31.1%
- his 6.1%
- a 3.1%
- behind 2.9%
- him 2.5%
- her 2.4%
- under 1.6%
- their 1.6%

Cycle structure of *abc*-permutations

We fully characterize the cycle structure of *abc*-permutations.

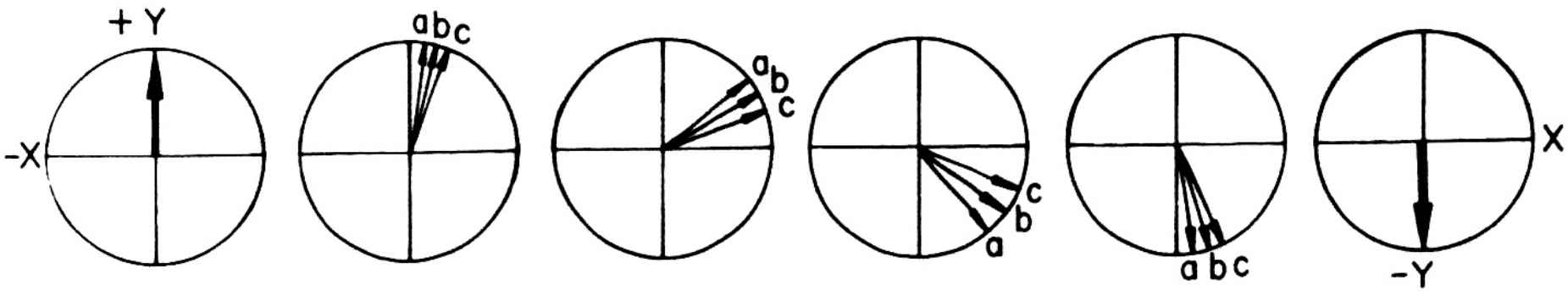
Cycle structure and pattern avoidance of *abc*-permutations

Sally Wolfe

July 30, 2010

Spin Echoes

- Measuring relaxation directly has problems
  - Proximity to driving pulse
  - Inhomogeneity in static field alters observed T2
- Use 180° pulses to produce spin echoes (Hahn 1950)
  - Reverses phase decoherence from inhomogeneity



General Structure

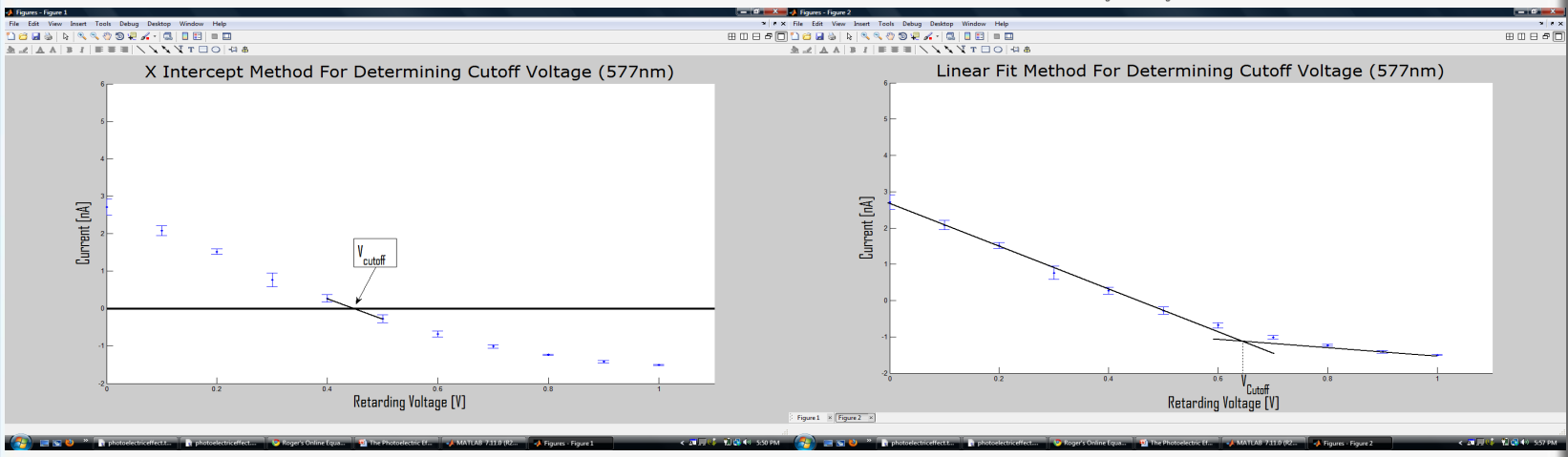
	Victor stands outside
Peggy: Prepare	Peggy vanishes into the cave
Peggy: Commit	Victor comes back in, . . .
Victor: Challenge	. . . and calls out which side Peggy should return by
Peggy: Respond	Peggy returns as requested

Finding the Cutoff Voltage

$$KE_{max} = h\nu - \Phi - eV_{retarding}$$

$$V_{cutoff} = \frac{h}{e}\nu - \frac{\Phi}{e}$$

Two Methods to determine $V_{cutoff} = \frac{h}{e}\nu - \frac{\Phi}{e}$



Spinner Assembly: Final Model

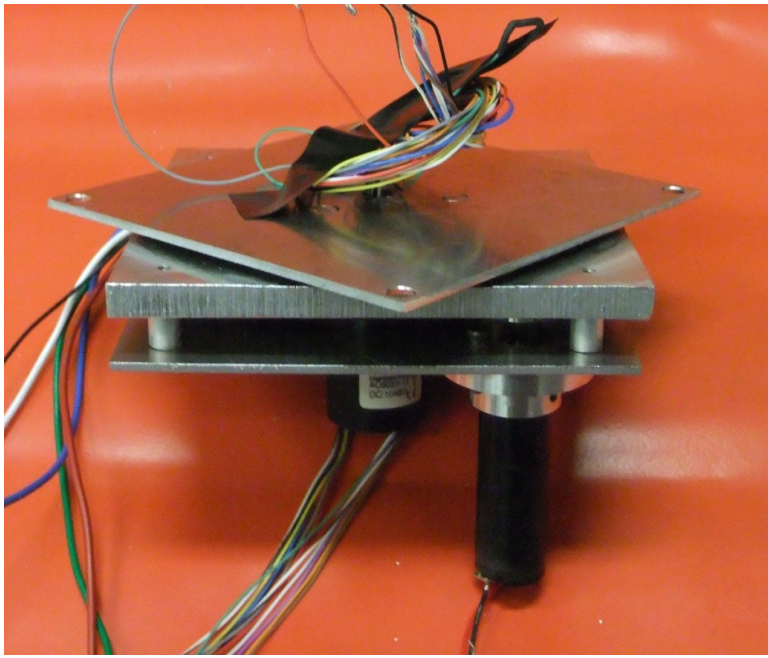
Specifications

Max Angular Velocity: 1.7 Hz

Motor Controller: Pololu QiK TTL Interface

Slip Ring Channels: 12

Dimensions (Interface Space): 100mm x 100mm x 18mm



History

- Compton's x-ray diffraction experiments (1920-2)
  - Wavelength shift in scattered radiation
  - Explanation using photon momentum
- Wilson, Bothe detect recoil electron (1923)
- Wave-particle duality (de Broglie, Schrödinger)

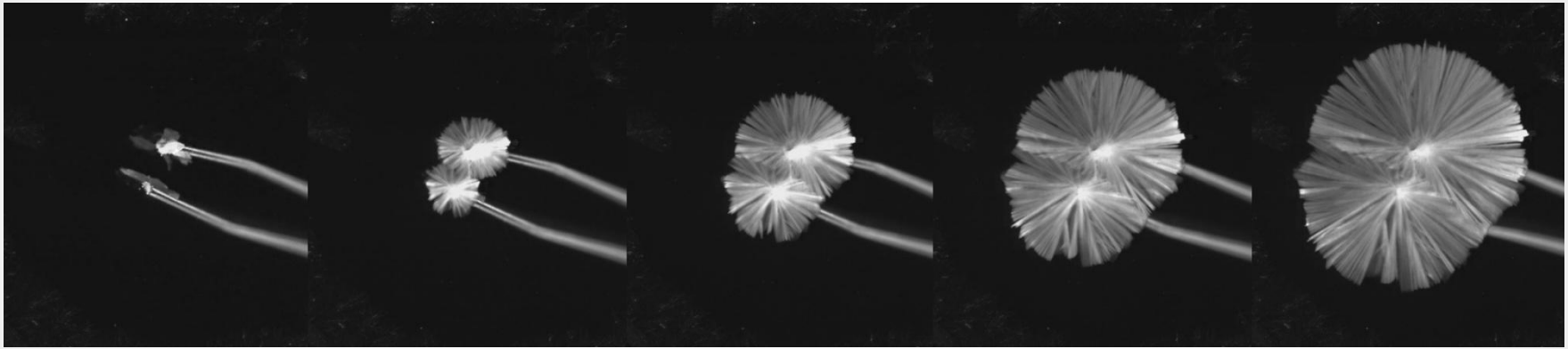
Ideas from the classification of cycle structure, cont

To show that each residue class contains exactly one residue class, we note that if x is in a cycle of length j, then

$$\sigma_{abc}^{j}(x) = x + m(a+b) - ld = x.$$

and $m + l \leq j$.

Results



Five frames of Sodium Acetate crystalizing from below. Each frame is .2 seconds apart, all five frames span .8 seconds. Shot at 1000 fps, f/8, 90mm lens.

What Skills Could Be Learned?

distributed collaboration

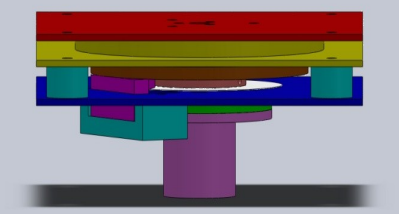
information management

organization navigation

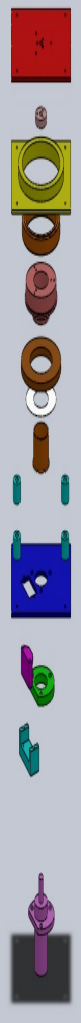
interagency coordination

cultural awareness

Spinner Assembly: Design Review



Not Shown:
- Micro DC Motor
- 15 Tooth Brass Gear 15mm PD
- Small Gear Mounting Collar
- Flexible Coupling



Payload Mounting Plate

Flexible Coupling

Attachment

Bearing Housing

Multi-Load Bearing

Hollow Shaft

65 Tooth Steel Gear 65mm PD

2500 Tick Encoder Disk

Insert

Spacers

Bus Cover Plate

Optical Encoder

Slip Ring Spacer

Encoder Mounting Bracket

Slip Ring

Compton Scattering and the Klein-Nishina Formula

Daniel J. Fremont

8.13
Massachusetts Institute of Technology

Spinner Assembly: Summary

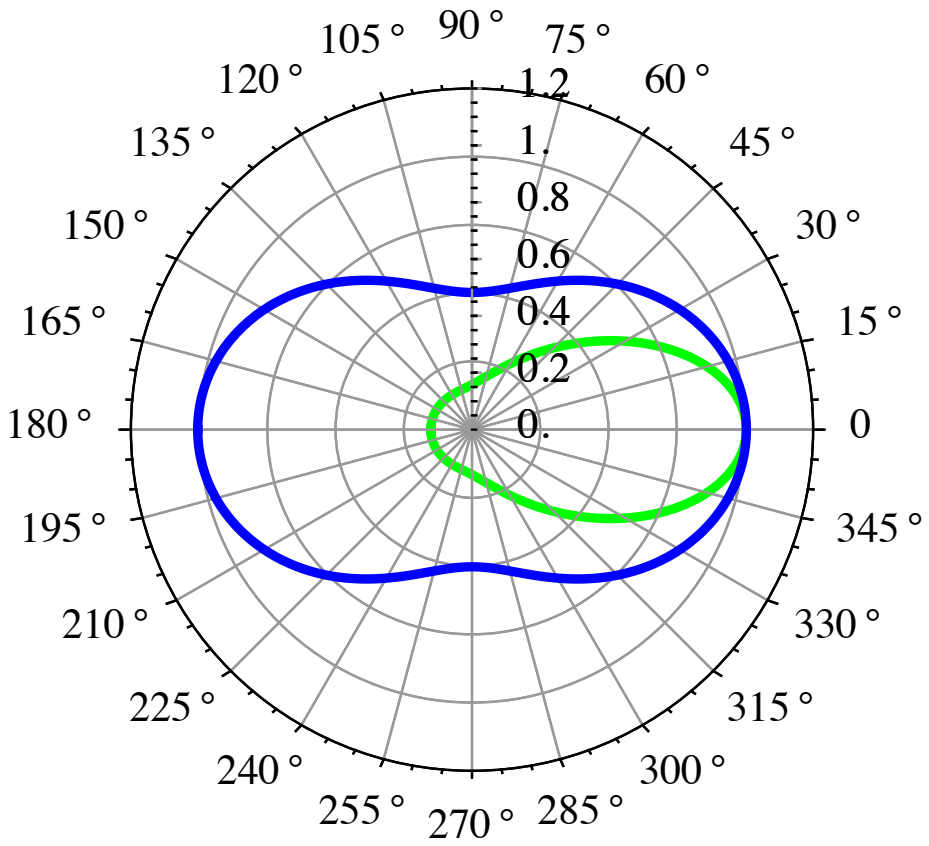
Spinner Assembly redesign was successful

Meets volume, data transmission and pointing knowledge requirements

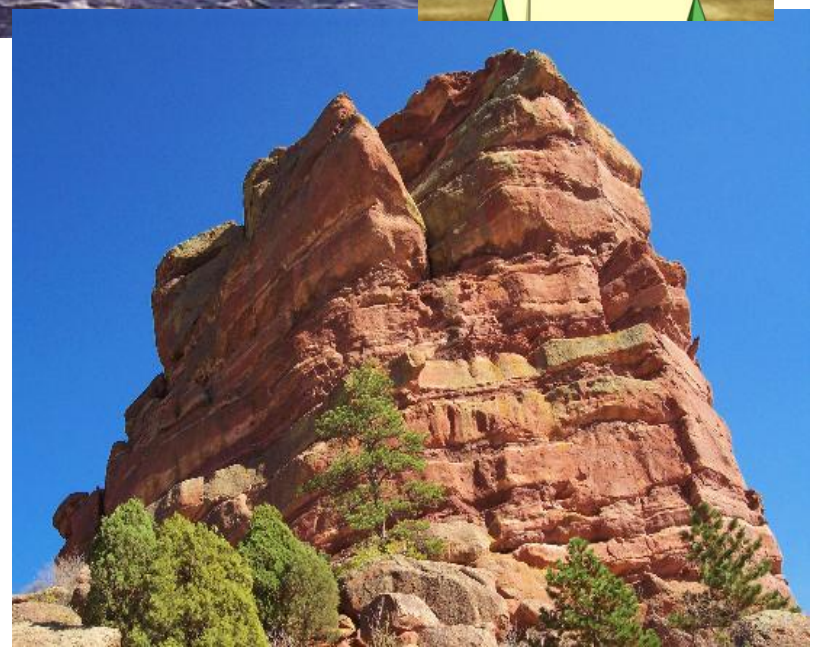
Next Step: Selection of Space Rated Components

Scattering Intensities

- Classical treatment: Thomson cross-section
  - Only valid for low energies
- Relativistic treatment: Klein-Nishina formula

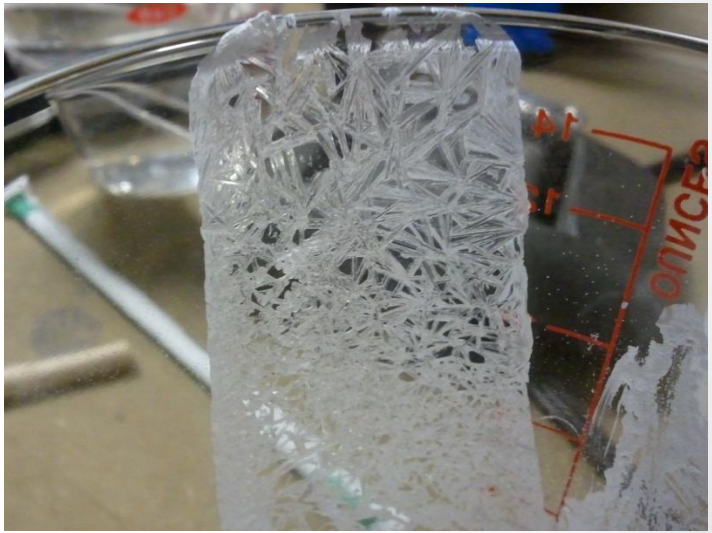


Rock



Background: sodium acetate

- Sodium acetate (NaAc) can perform rapid crystallization when supersaturated
- Supersaturation is when more solute than is normally possible is dissolved into a solvent
  - Can be achieved by increasing temperature
- If a supersaturated solution of NaAc is slowly cooled, it can be rapidly crystallized if perturbed or given a nucleation site



[1] http://jchemed.chem.wisc.edu/JCESoft/CCA/CCA3/MAIN/ACETATE/PAGE1.HTM

Sodium Acetate

Stable supersaturated solutions crystallize when seed is introduced

Browser security

- Webpages are very restricted
  - Cannot read your English paper
  - Cannot write a virus
  - Cannot delete your files
- Visiting evil.example.com should be safe
- Browser enforces these restrictions
- What if there is a bug?

Spinner Assembly: Qualitative Testing

Results:

Noticeable signal distortion appears at frequencies >1 KHz

Significant signal distortion appears at signal frequencies >1 MHz

Conclusion:

5 MHz Sine Wave serial

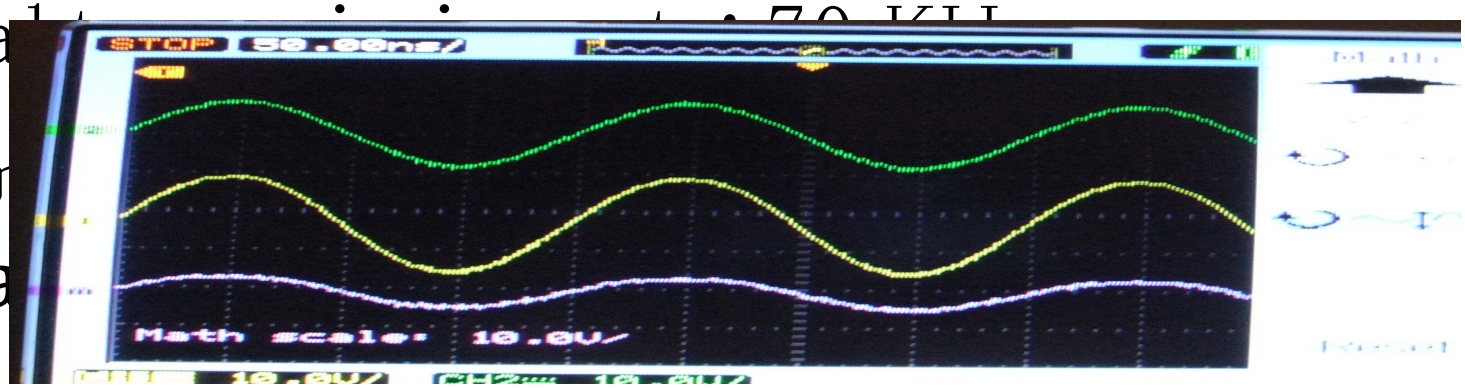
Transmitted Signal

Problem

Input

minima

Difference

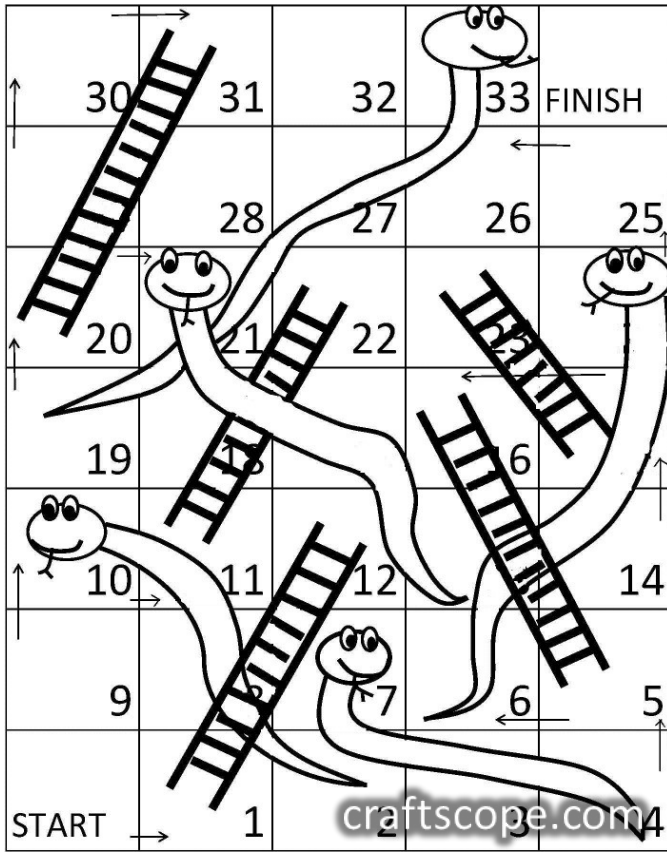


Professor Dumbledore knew something extremely odd stuff I'm going to feed the lake and Lies "Isn't it?"

Markov chain

(the next thing you do depends only on the last few things you did)

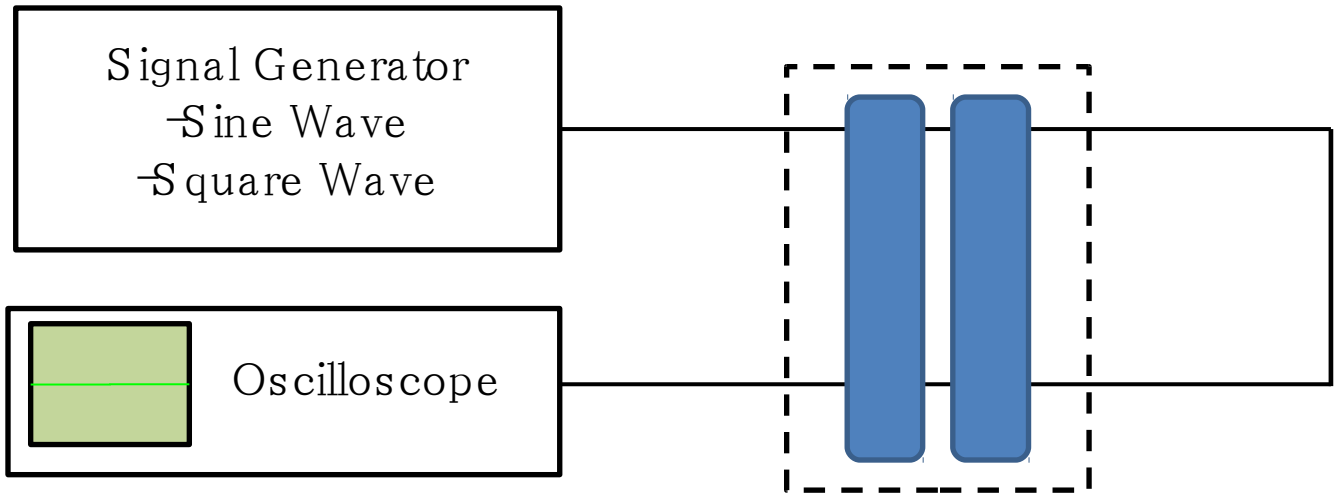
(in other words, you *forget* where you were before)



Markov chains: *forgetful* models

Spinner Assembly: Qualitative Testing

Setup:

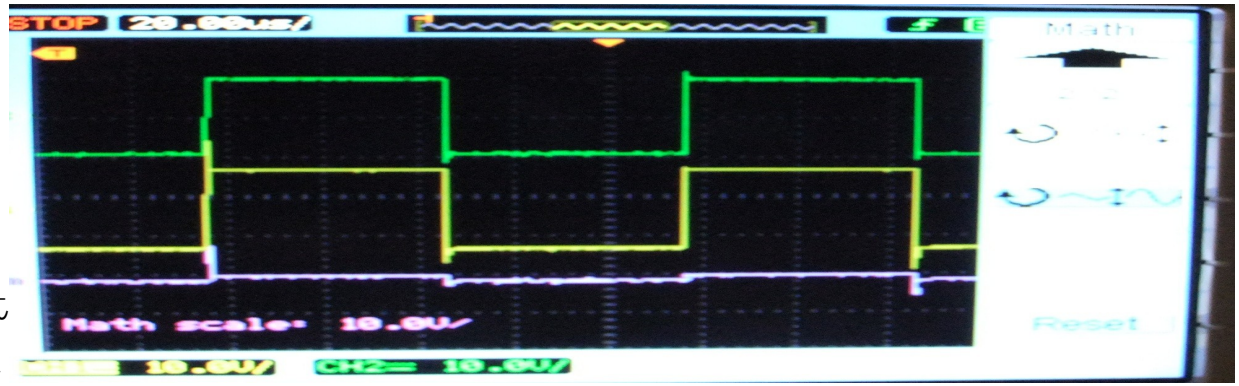


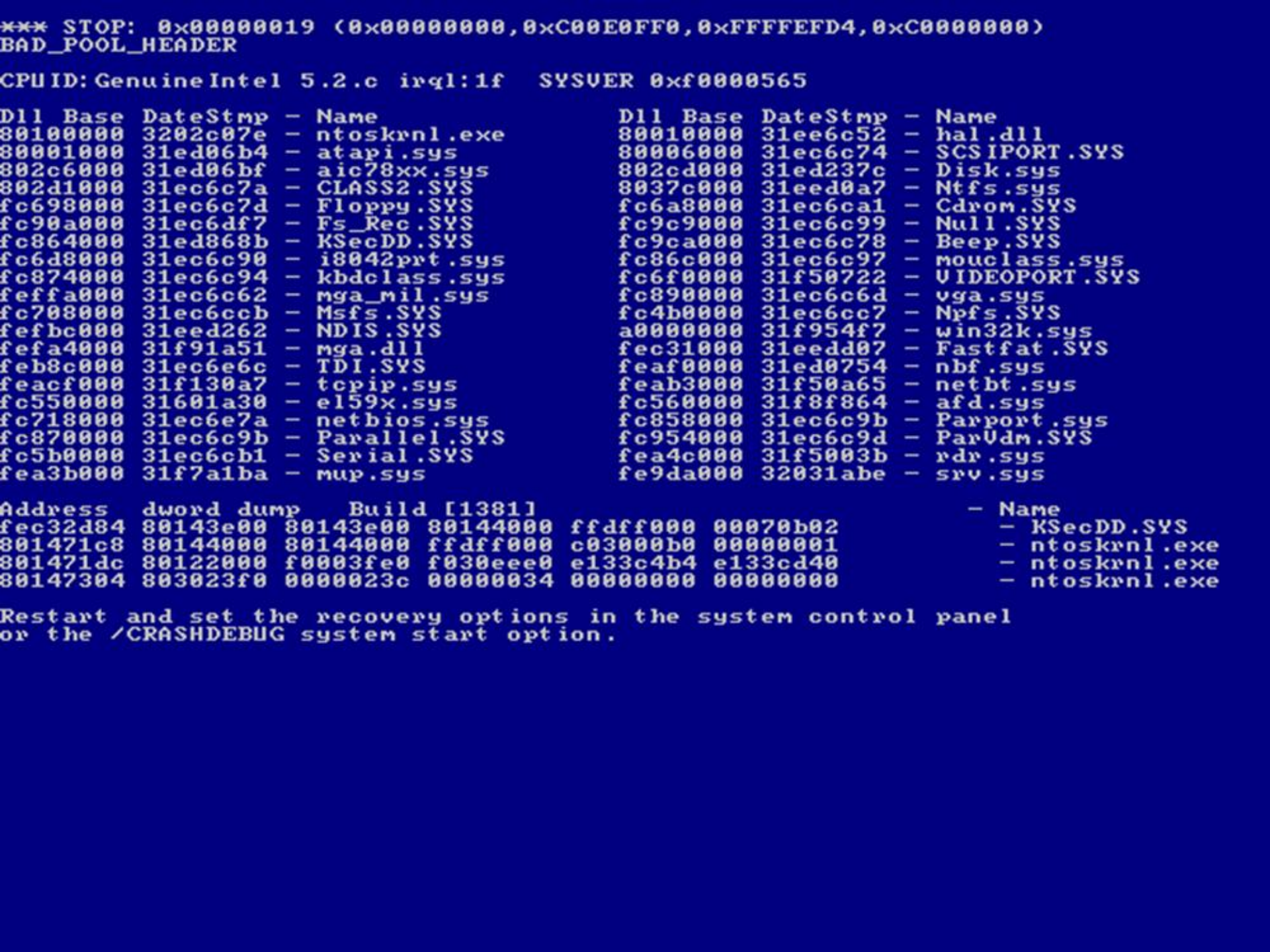
Spinner Assembly rotating at 1.7Hz

Sample Square Wave Output (10 Volts/div, 1kHz):

Transmitted Signal

Input Difference




*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER
CPUID:GenuineIntel 5.2.c irql:1f SYSVER 0xf0000565
Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe
80001000 31ed06b4 - atapi.sys
802c6000 31ed06bf - aic78xx.sys
802d1000 31ec6c7a - CLASS2.SYS
fc698000 31ec6c7d - Floppy.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS
fc864000 31ed868b - KSecDD.SYS
fc6d8000 31ec6c90 - i8042prt.sys
fc874000 31ec6c94 - kbdclass.sys
feffa000 31ec6c62 - mga_mil.sys
fc708000 31ec6ccb - Msfs.SYS
fefbc000 31eed262 - NDIS.SYS
fefa4000 31f91a51 - mga.dll
feb8c000 31ec6e6c - TDI.SYS
feacf000 31f130a7 - tcpip.sys
fc550000 31601a30 - el59x.sys
fc718000 31ec6e7a - netbios.sys
fc870000 31ec6c9b - Parallel.SYS
fc5b0000 31ec6cb1 - Serial.SYS
fea3b000 31f7a1ba - mup.sys
Dll Base DateStmp - Name
80010000 31ee6c52 - hal.dll
80006000 31ec6c74 - SCSIPORT.SYS
802cd000 31ed237c - Disk.sys
8037c000 31eed0a7 - Ntfs.sys
fc6a8000 31ec6ca1 - Cdrom.SYS
fc9c9000 31ec6c99 - Null.SYS
fc9ca000 31ec6c78 - Beep.SYS
fc86c000 31ec6c97 - mouclass.sys
fc6f0000 31f50722 - VIDEOPORT.SYS
fc890000 31ec6c6d - vga.sys
fc4b0000 31ec6cc7 - Npfs.SYS
a0000000 31f954f7 - win32k.sys
fec31000 31eedd07 - Fastfat.SYS
feaf0000 31ed0754 - nbf.sys
feab3000 31f50a65 - netbt.sys
fc560000 31f8f864 - afd.sys
fc858000 31ec6c9b - Parport.sys
fc954000 31ec6c9d - ParVdm.SYS
fea4c000 31f5003b - rdr.sys
fe9da000 32031abe - srv.sys
Address dword dump Build [1381] - Name
fec32d84 80143e00 80143e00 80144000 ffdff000 00070b02 - KSecDD.SYS
801471c8 80144000 80144000 ffdff000 c03000b0 00000001 - ntoskrnl.exe
801471dc 80122000 f0003fe0 f030eee0 e133c4b4 e133cd40 - ntoskrnl.exe
80147304 803023f0 0000023c 00000034 00000000 00000000 - ntoskrnl.exe
Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.

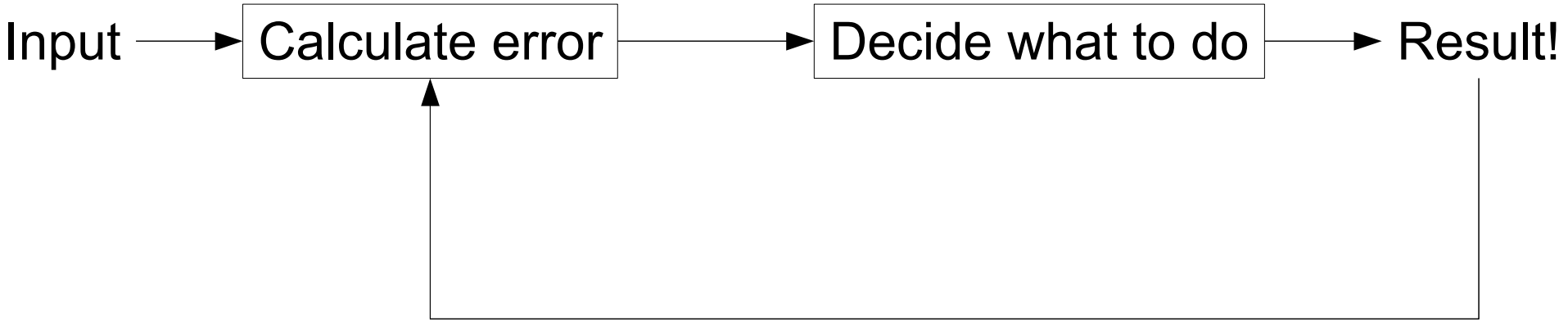
Questions?

- History of NMR
- Pulsed NMR
- Spin-Lattice and Spin-Spin Relaxation
- Spin Echoes
- Proton Larmor Frequency
- Effects of Fe^{3+} ions on Relaxation Times

COMPUTER

Y U NO UNDERSTAND ENGLISH

Feedback



Definition of $\mathbf{p}_k(n)$

Since

$$\mathbf{p}(n) = 1 - \sum_{s=2}^{n} \mu(s) f(n, s),$$

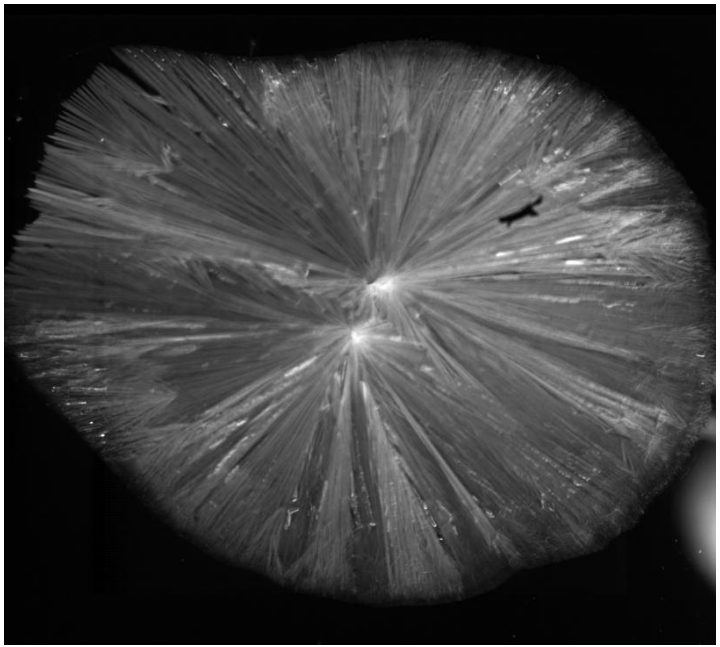
we have

Theorem

$$\mathbf{p}_k(n) = \begin{cases} f(n,k)(1 - \sum_{s=2}^{n/k} \mu(s) f(n/k, s)) & \text{if } n \mid k \\ f(n,k)(1 - \sum_{s=2}^{n/k} \mu(s) \Gamma(n/k, s)) & \text{if } n \nmid k \end{cases}$$

where $\Gamma(n,k)$ *is a similar function to* $f(n,k)$.

High Speed Crystallization



Crystallization of supersaturated Sodium Acetate solution from below. The two points of emanation caused by two seeds are clearly visible. Shot at 1000 fps, f/8, 90mm lens.

Idea of the construction of $\mathbf{p}_k(n)$, cont

Then

$$\mathbf{p}_k(n) = f(n,k) \cdot Pr(B_k \text{ given } A_k).$$

If $n \mid k$, we have that $k \mid (a+b)$ and $(b+c)$ implies that $k \mid a, b, c$. Then choosing the blocks a, b, c partitioning n is equivalent to choosing blocks $a/k, b/k, c/k$ partitioning n/k.

Discussion: moving forward

With sodium acetate:

- vary temperature/concentration, look at linear crystallization speed (see 1957 paper)
- look at types/processes of crystallization

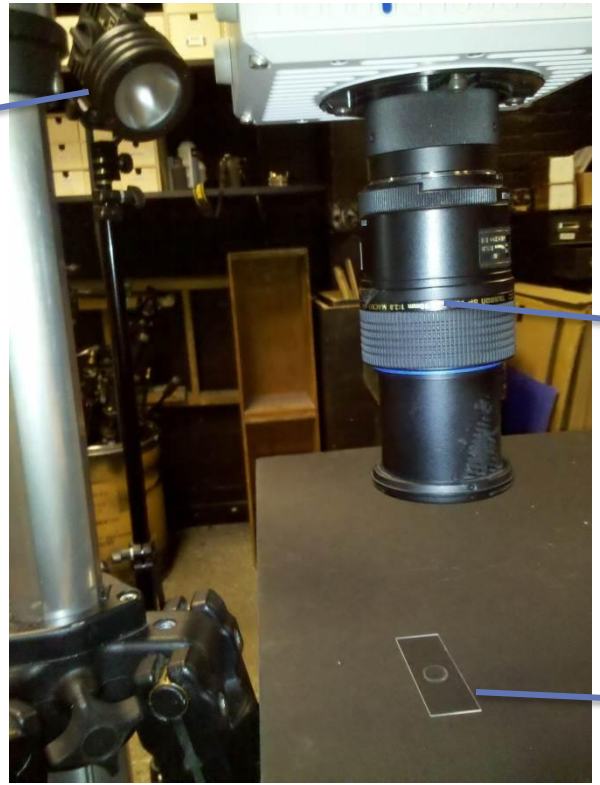
Google PageRank

- Internet contains N web pages
- Page contains k links
- Follow a link or type a URL
- Model as a Markov chain
- What pages do users end up on?
- Higher ad prices, earlier search results

History of NMR

- Rabi (1937) predicts and first observes NMR
- Purcell and Bloch (1945) measure relaxation times and their dependence on chemical properties
- Chemical shifts discovered (1950-1)
- Lauterbur (1973) applies NMR to medical imaging

Procedure: overhead setup



Discussion: conclusions

- Sodium Acetate is feasible
  - Crystallizes consistently and on recordable time scales

- Bismuth isn't feasible
  - Crystallization isn't happening on time/physical scales we have the techniques to record

Ideas from the classification of cycle structure, cont

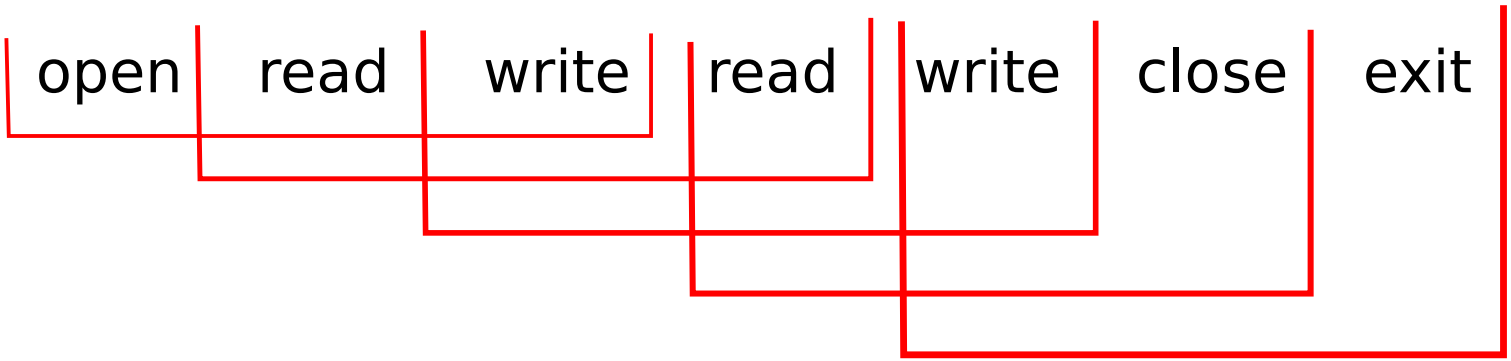
Therefore, for all i and x we have

$$\sigma_{abc}^{i}(x) = x + m(a+b) - ld.$$

for some integers m, l satisfying $|m| + |l| \leq i$.

Prior Art: stide

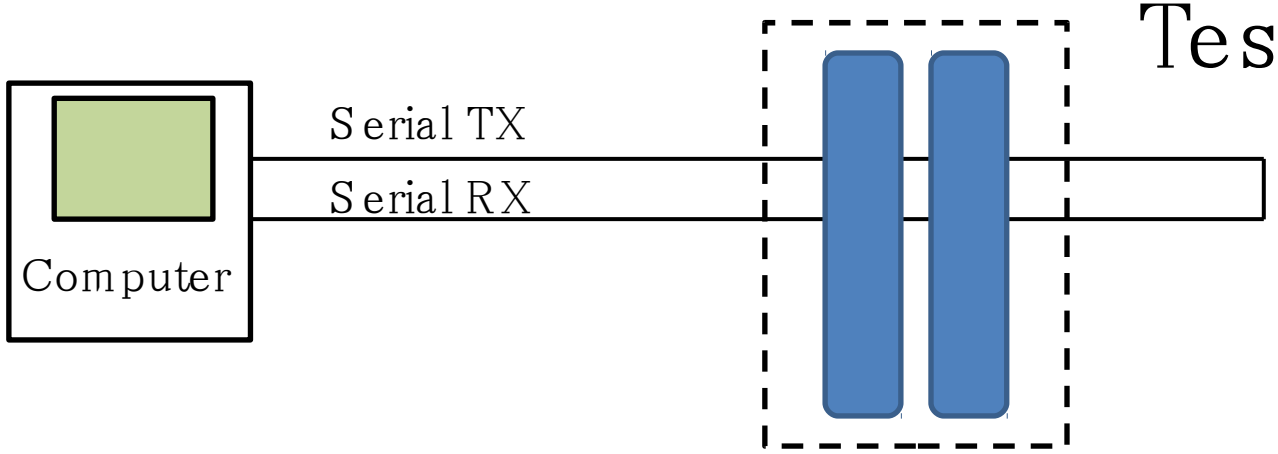
- Sequence Time-Delay Embedding
- Sequences (*n*-grams) of syscalls



- Look at rolling window of twenty sequences at a time. If enough of them are unknown, alert.

Spinner Assembly: Quantitative Testing

Setup:



Spinner Assembly rotating at 1.7 Hz

Results:

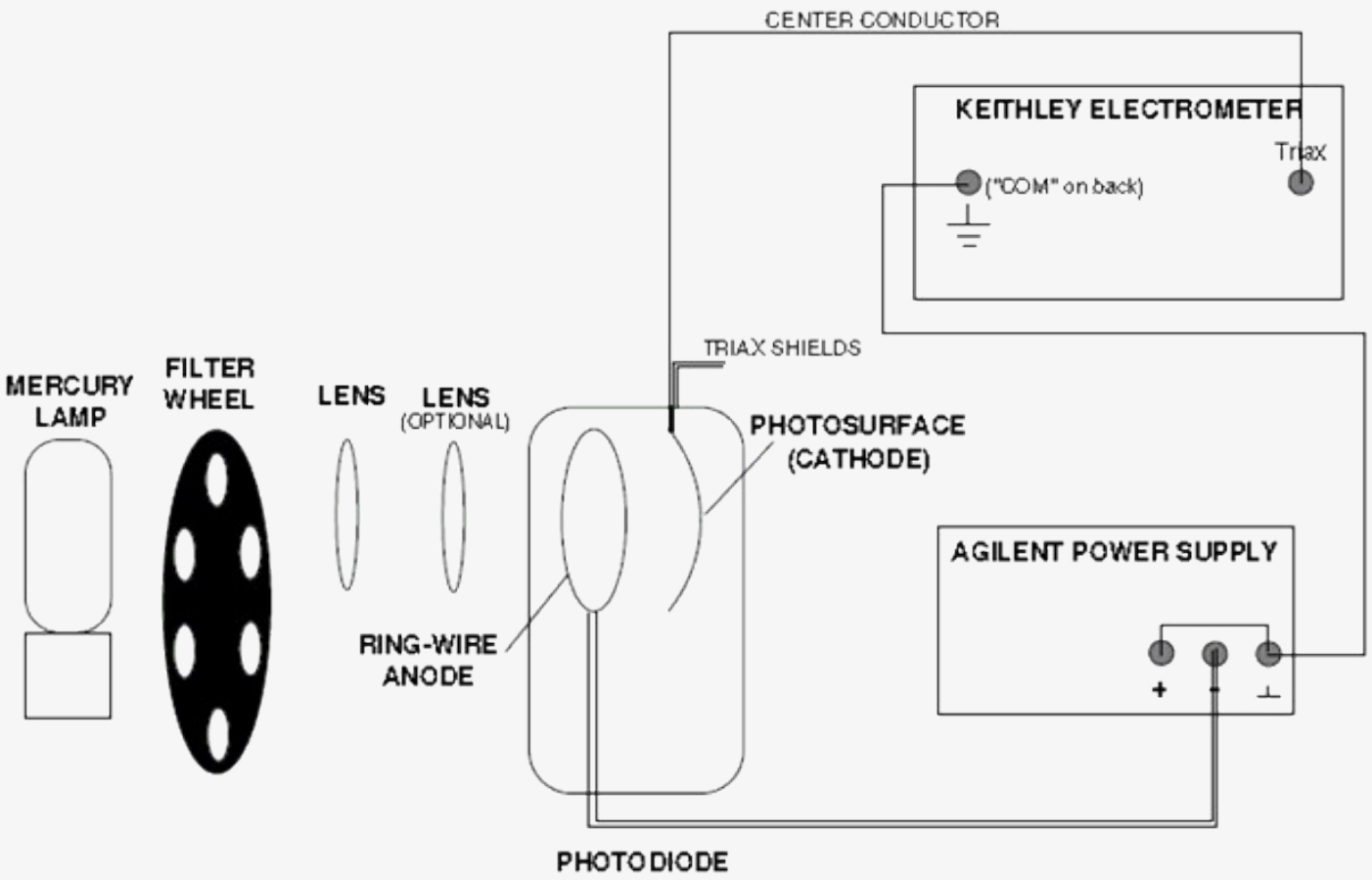
1,000,000 bytes sent; 0 errors

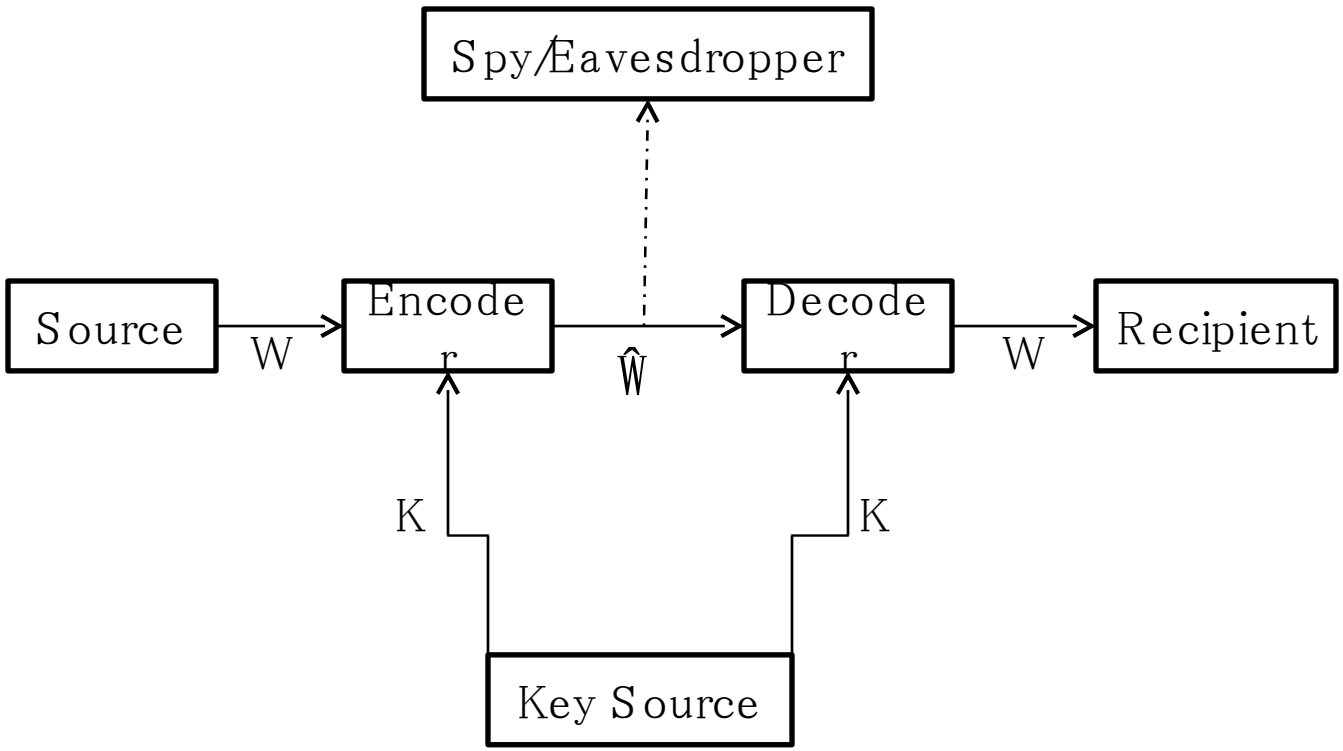
Error probability < 0.0000054 with 99% confidence

Conclusion:

Slip ring interface is suitable for serial data

Experimental Setup




Spy/Eavesdropper
Source
W
Encoder
Decoder
Recipient
W
K
K
Key Source

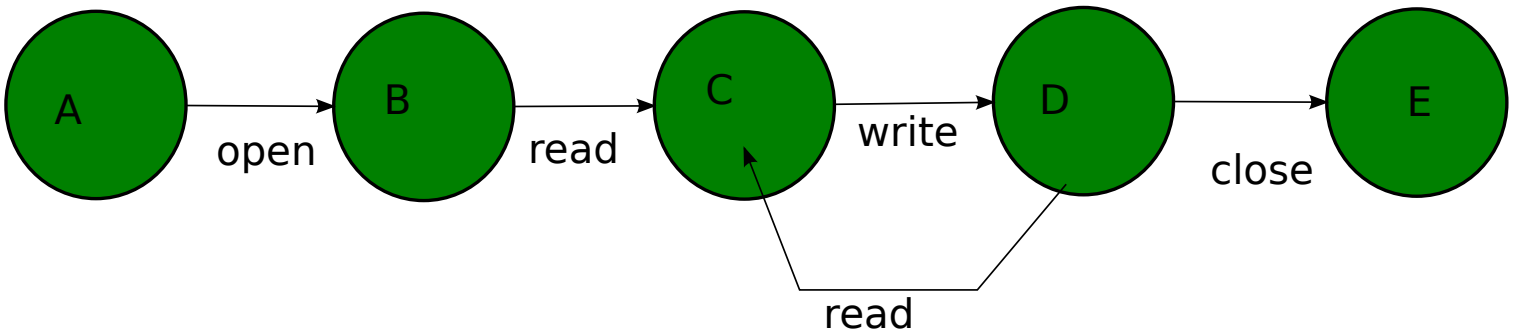
Summary

- $h = (6.348 \pm 0.0626) \cdot 10^{-34}\ \mathrm{J \cdot s}$
- $\phi = 1.76 \pm 0.026\ \mathrm{eV}$
- Photoelectric effect well described by Einstein's model
  - Linear dependence of cutoff voltage on frequency
- Particle-like nature of light

Questions?

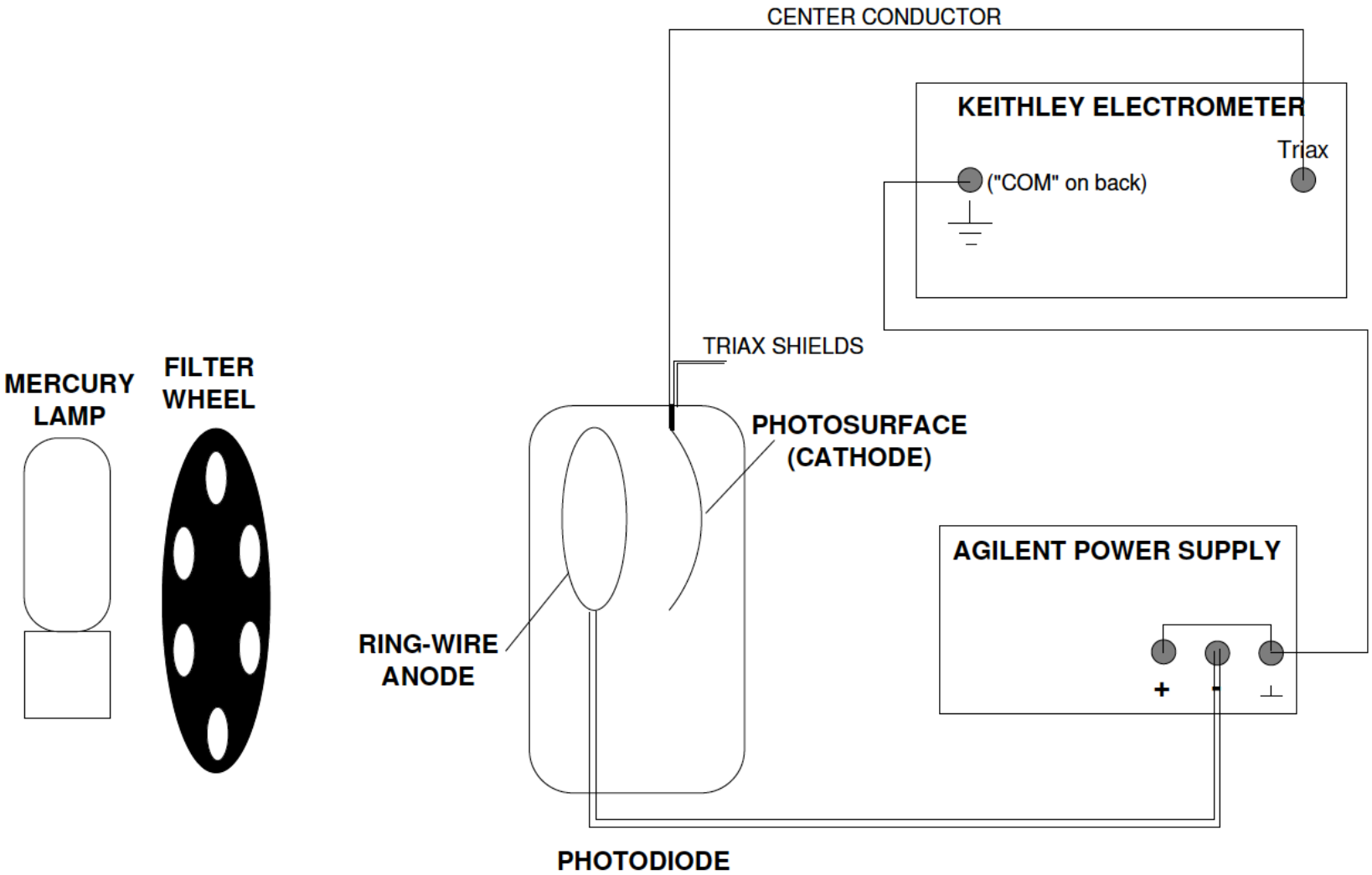
Prior Art: Finite Automata

- Maintain current "state" associated with the syscalls so far (and other info)
- Define transitions between the various states
- When the appropriate syscall is seen, transition to the appropriate new state:



- If an unfamiliar syscall is made, alert

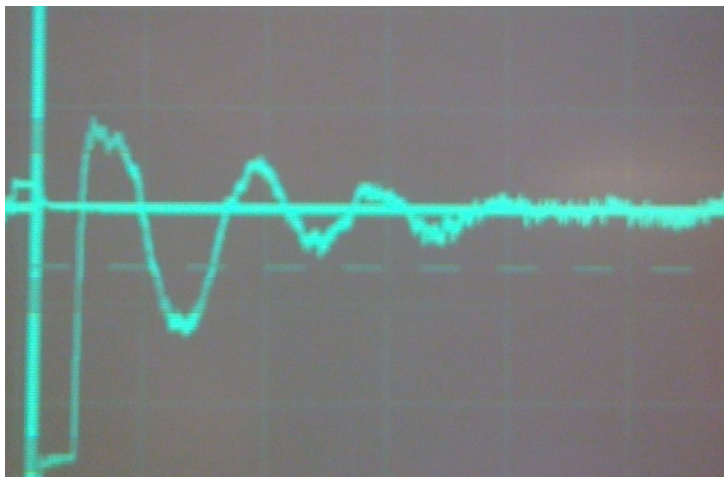
Experiment Setup

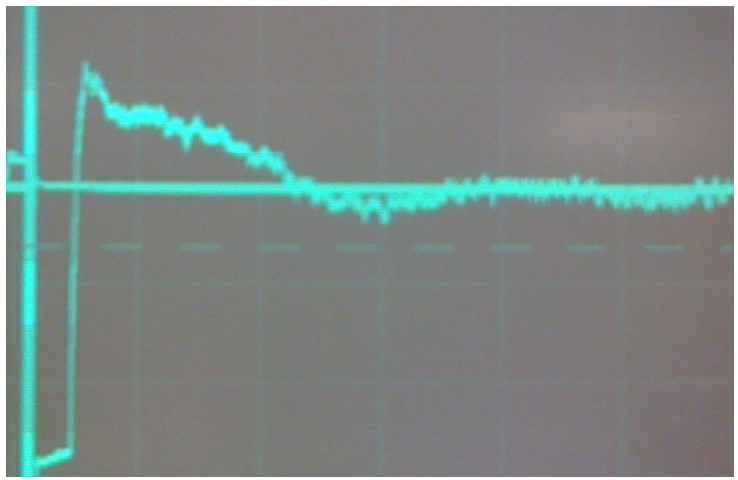


Slightly modified from experiment lab guide (`http://web.mit.edu/8.13/www/intro2.shtml`).

Finding Resonance

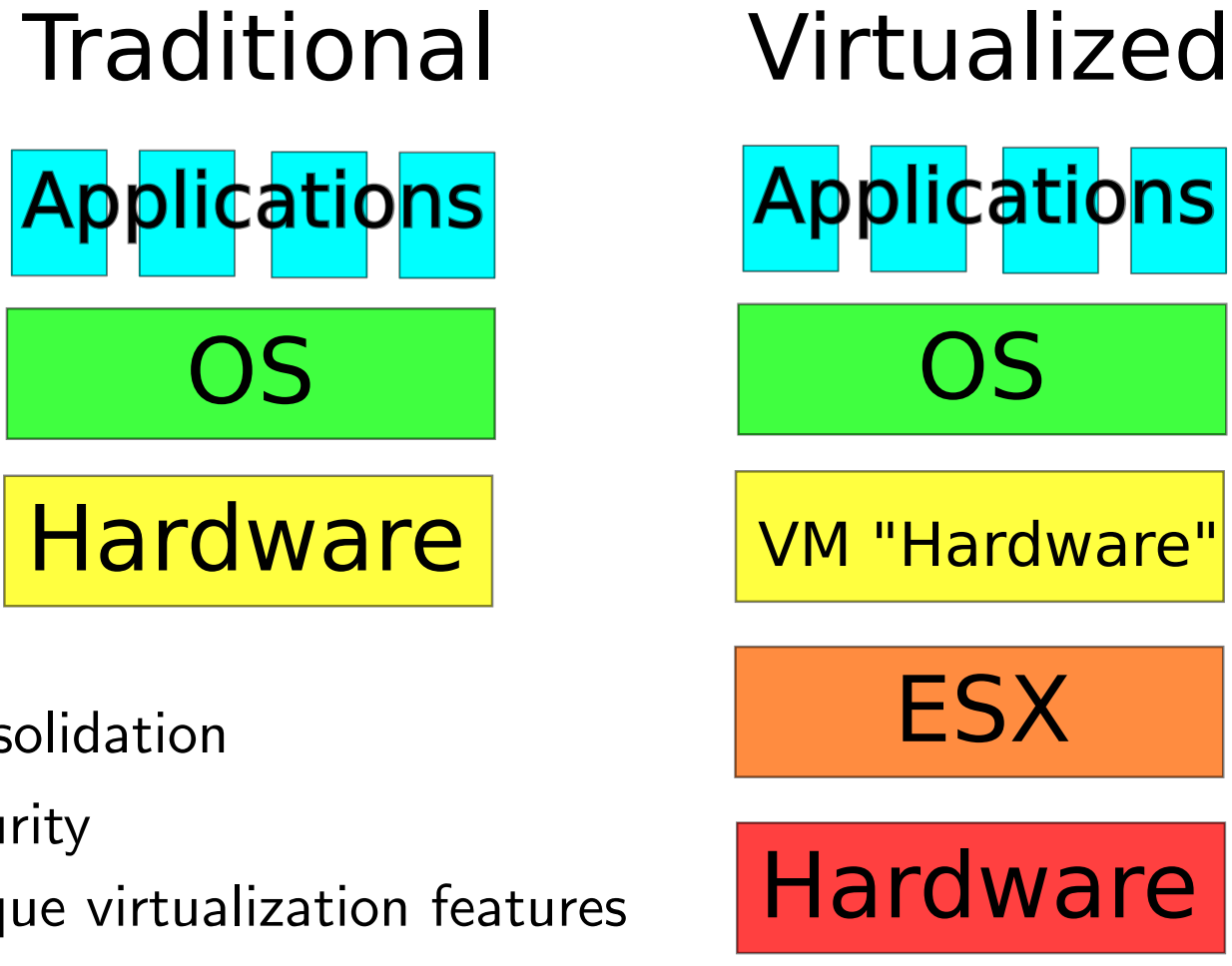
- Minimize beats
  - $\nu_{beats} = |\nu_{pulses} - \nu_{Larmor}|$





- Find most uniform B field
  - Inhomogeneity $\rightarrow$ different resonances $\rightarrow$ weaker signal
- Result: $(1.424 \pm 0.083) \cdot 10^{-26}$ J/T (3% off accepted value)

Virtualization



- Consolidation
- Security
- Unique virtualization features

Summary

- Systematic errors in amplitude data too large to allow verification of Klein-Nishina, but data definitely inconsistent with classical prediction
- Attenuation data strongly supports Klein-Nishina result over Thomson
- Necessity of relativistic quantum description of photons and electrons

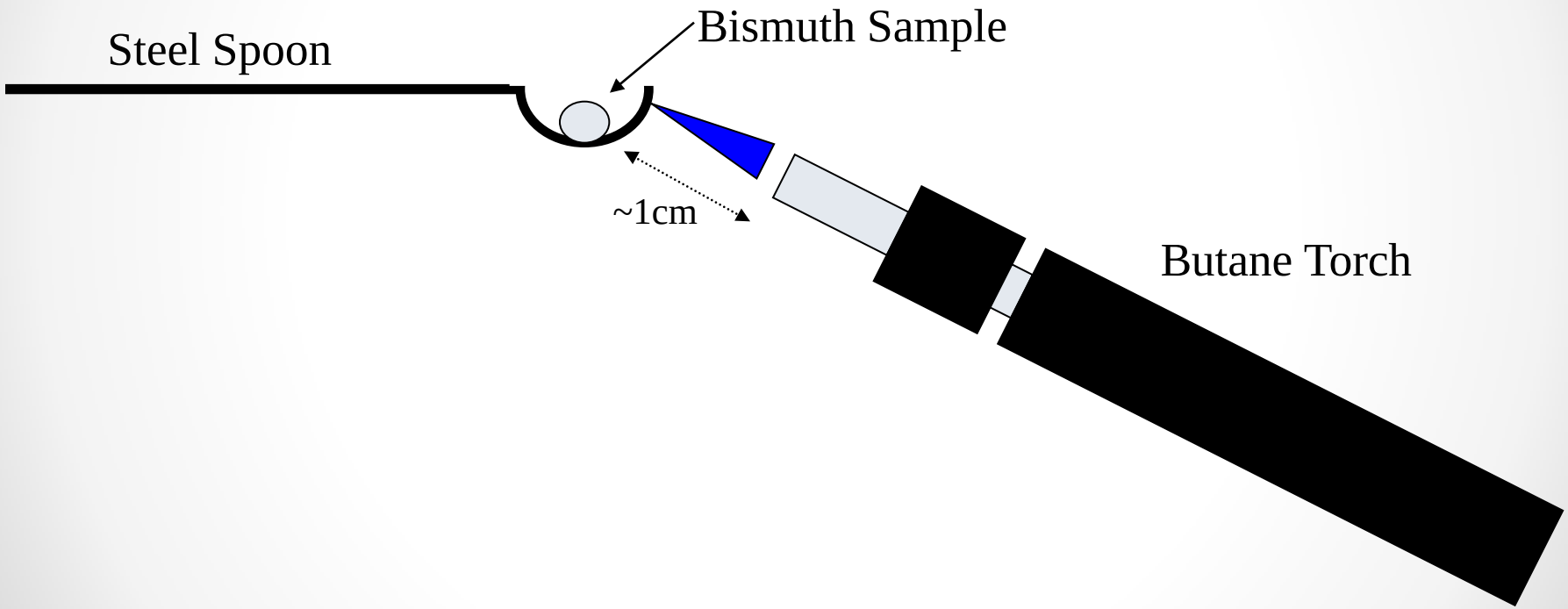
Spin-Lattice Relaxation (T1)

- Return of spins to thermal equilibrium
- Energy transferred into molecular motions
- Lattice frequencies must be close to Larmor frequency

Playing in the sandbox

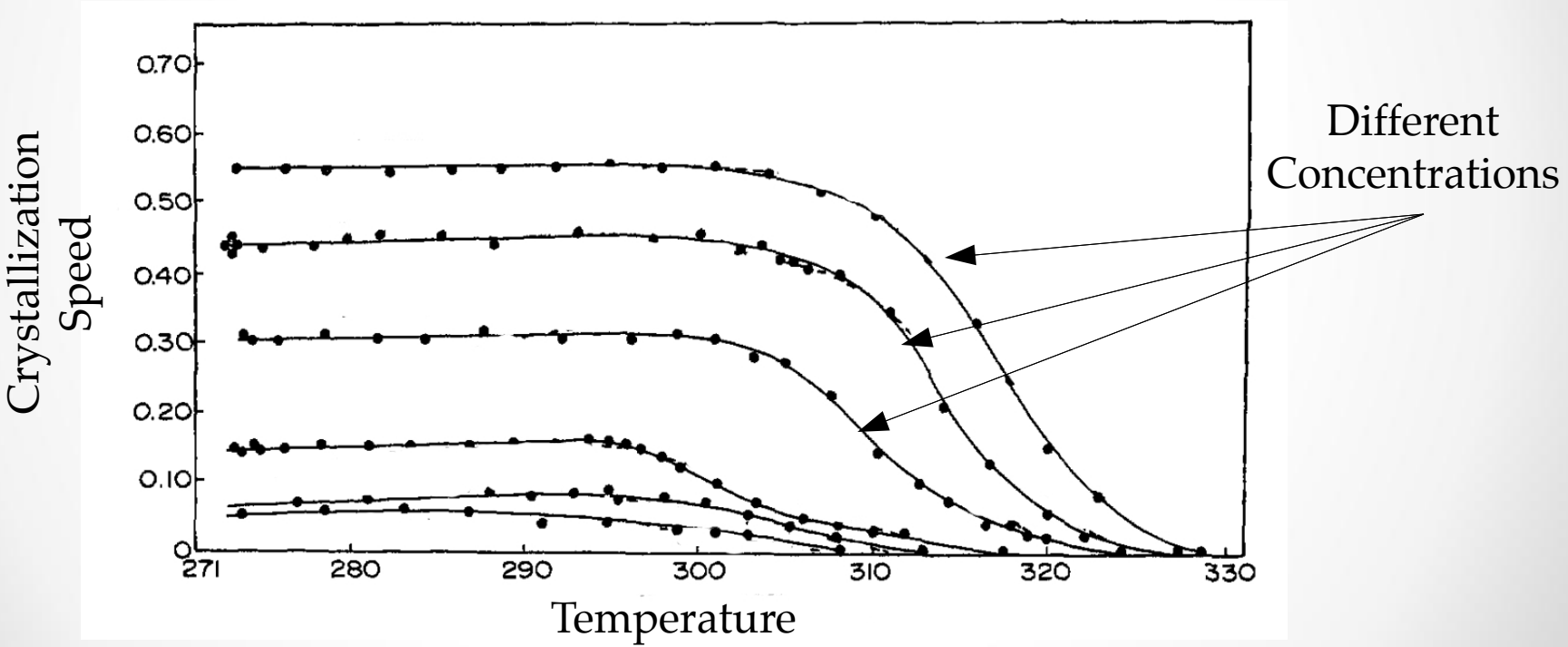
- How tab isolation works
- Sandboxing
- Principle of least privilege

Procedure: bismuth setup



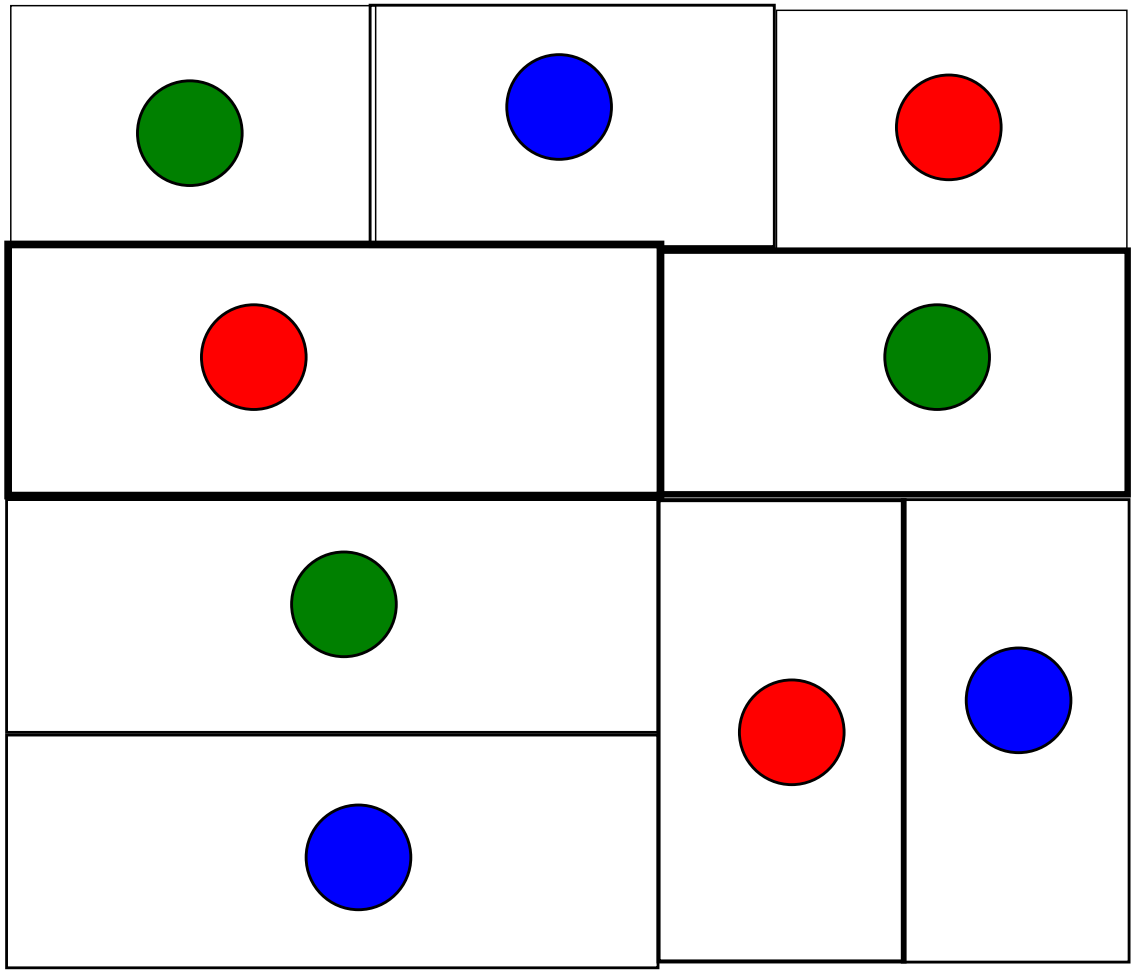
Previous Work

- Dietz, Bruckner, and Hollingsworth (1957)

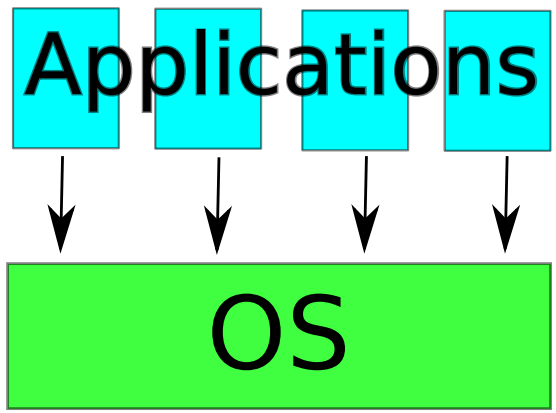


Map coloring ZKP

Prepare



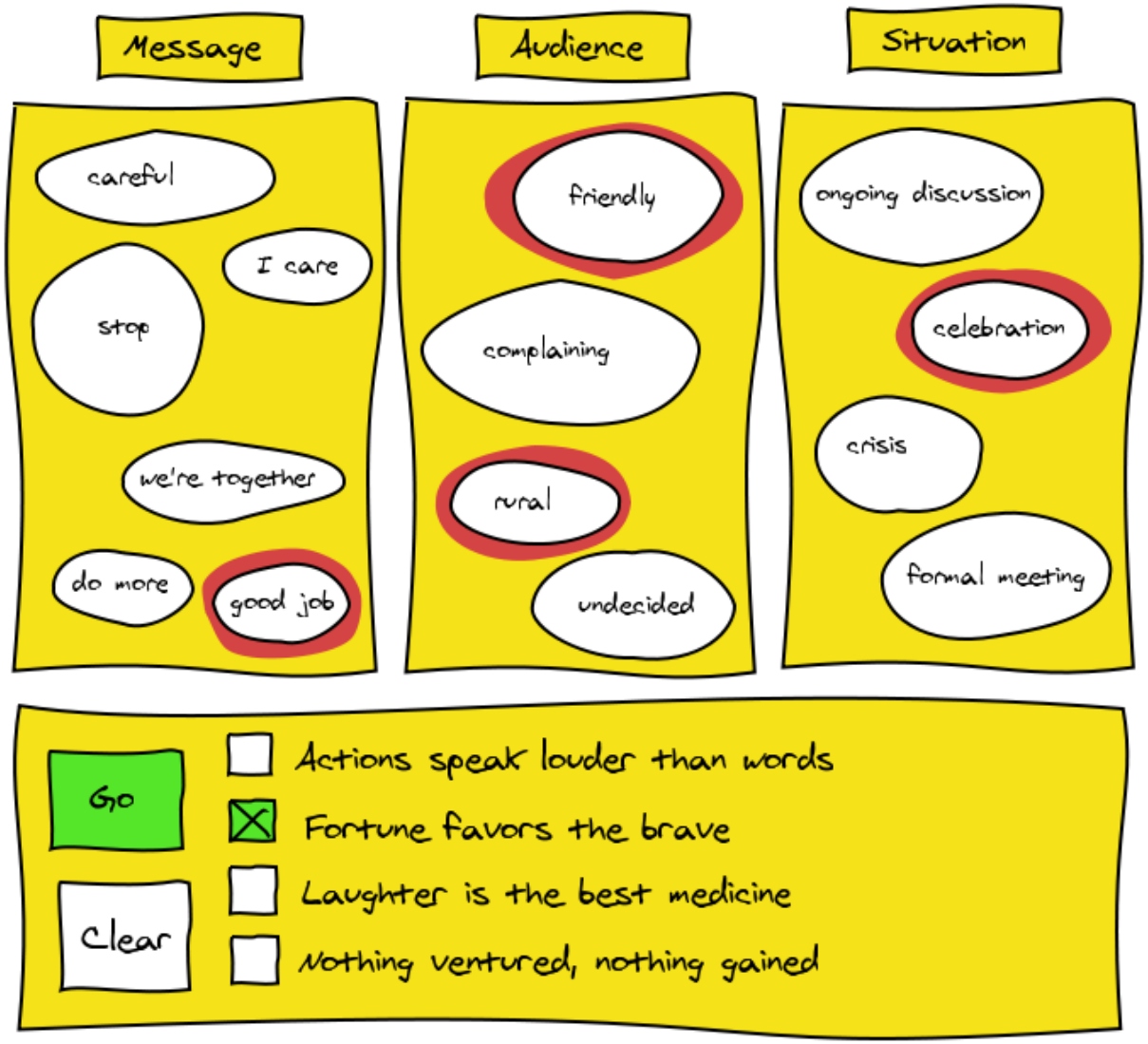
vprobes IDS



Watch interface between apps and OS

- Use vprobes to watch application/OS communication
- Build a profile of normal behavior
- Alert when abnormal behavior occurs

Finding Possible Proverbs



Attenuation Results

- Measured electron cross-section: $(2.50 \pm 0.025) \cdot 10^{-29}\ m^2$
  - Klein-Nishina prediction: $2.56 \cdot 10^{-29}\ m^2$ ($\approx 2\,\sigma$ off)
  - Thomson prediction: $6.65 \cdot 10^{-29}\ m^2$ ($\approx 166\,\sigma$ off!)
- Small systematic error
  - Some scattered photons detected
  - Detector drift
- Relativistic effects dominant: Klein-Nishina model much more accurate than classical Thomson model

What do we mean by “innovation”?
Purpose driven creativity

An abstract sculpture?

Creative.

An abstract sculpture that prevents the wind from spinning a building’s revolving doors too fast?

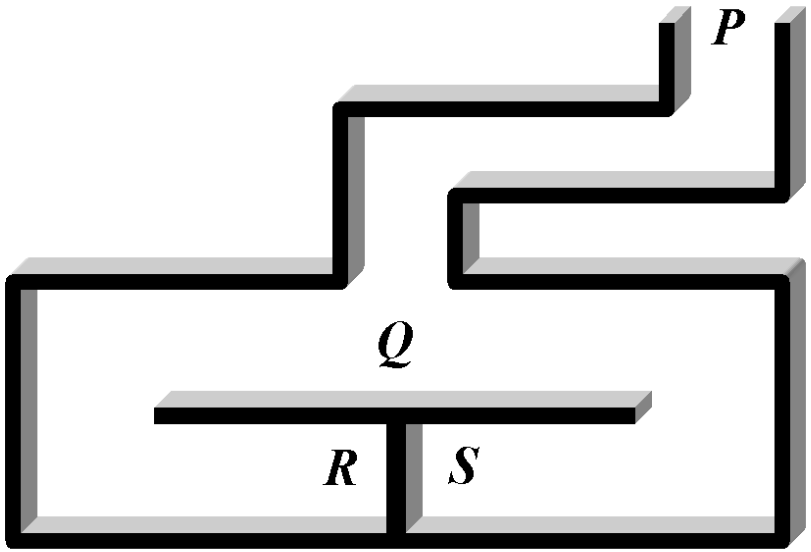
Innovative.

Summary

- Observed NMR in protons at the expected frequency
- Verified expected effects of Fe^{3+} ions on relaxation times
- Suggested usefulness of NMR in chemical analysis

Solution

- Victor stands outside at P
- Peggy vanishes into the cave and stands at R or S
- Victor comes back in, stands at Q, and calls out which side Peggy should return by
- Peggy returns as requested



General Structure

	Victor stands outside
Peggy: Prepare	Peggy vanishes into the cave
Peggy: Commit	Victor comes back in, . . .
Victor: Challenge	
Peggy: Respond	

Zero-Knowledge Proofs

Goal: Peggy (prover) wants to convince Victor (verifier) of something

Convincing If true, an honest prover can always convince an honest verifier

No cheating If false, a dishonest prover can only rarely convince an honest verifier

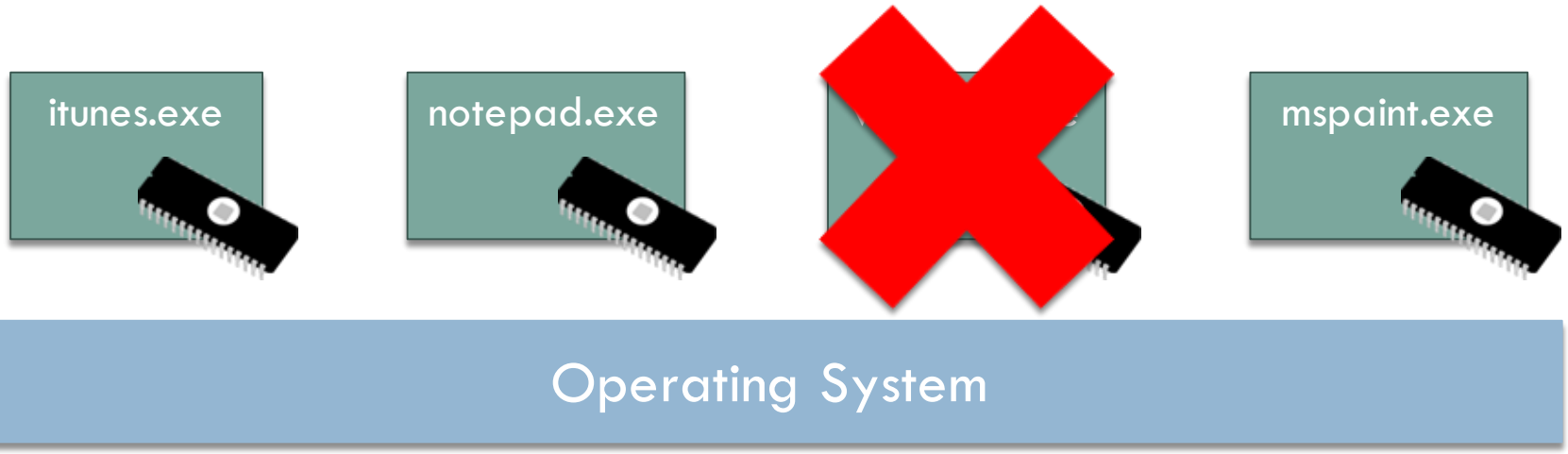
Zero knowledge If true, a cheating verifier cannot learn anything more than that it is true.

Stabilizing unstable systems: balance and levitation

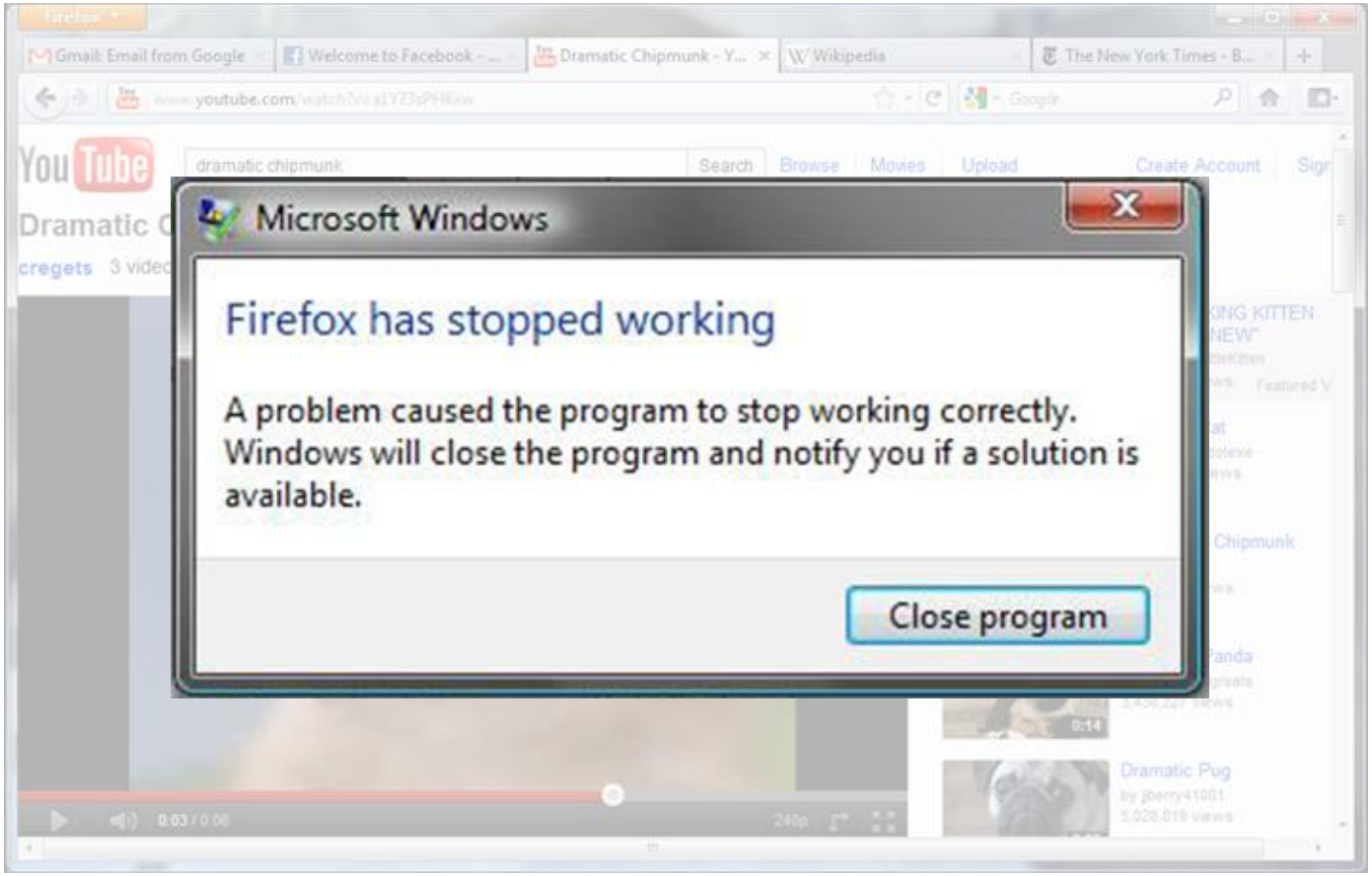
Sally Wolfe

Processes

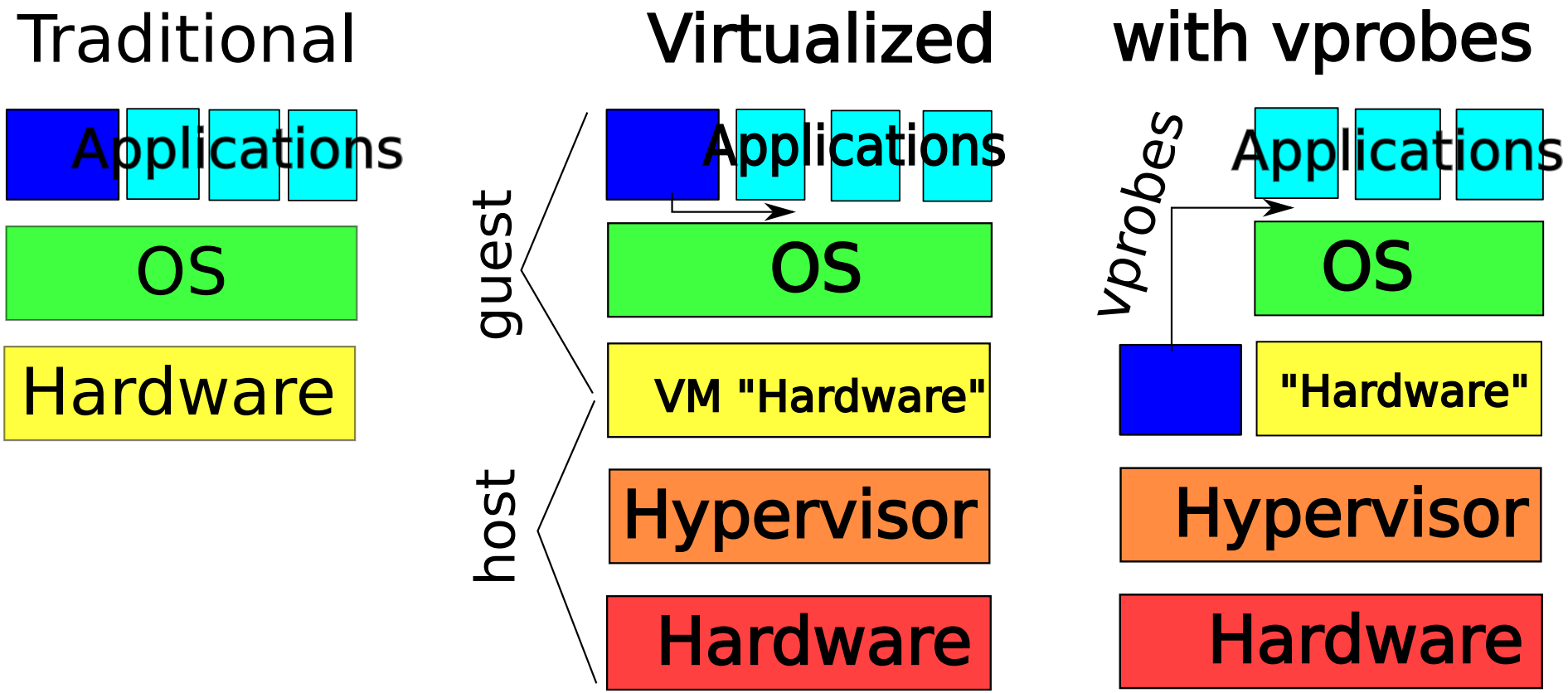
- Tasks organized into processes
- Typically one process per application
- Each process has private memory, state, etc.
- Independently scheduled and killed



What if a webpage crashes?



How can virtual machines help?

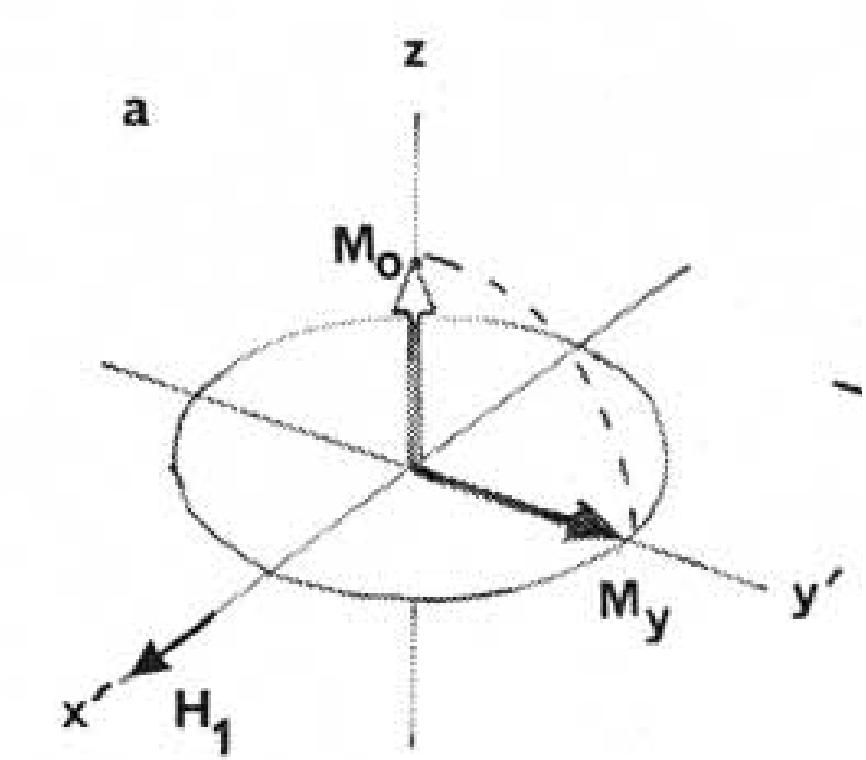


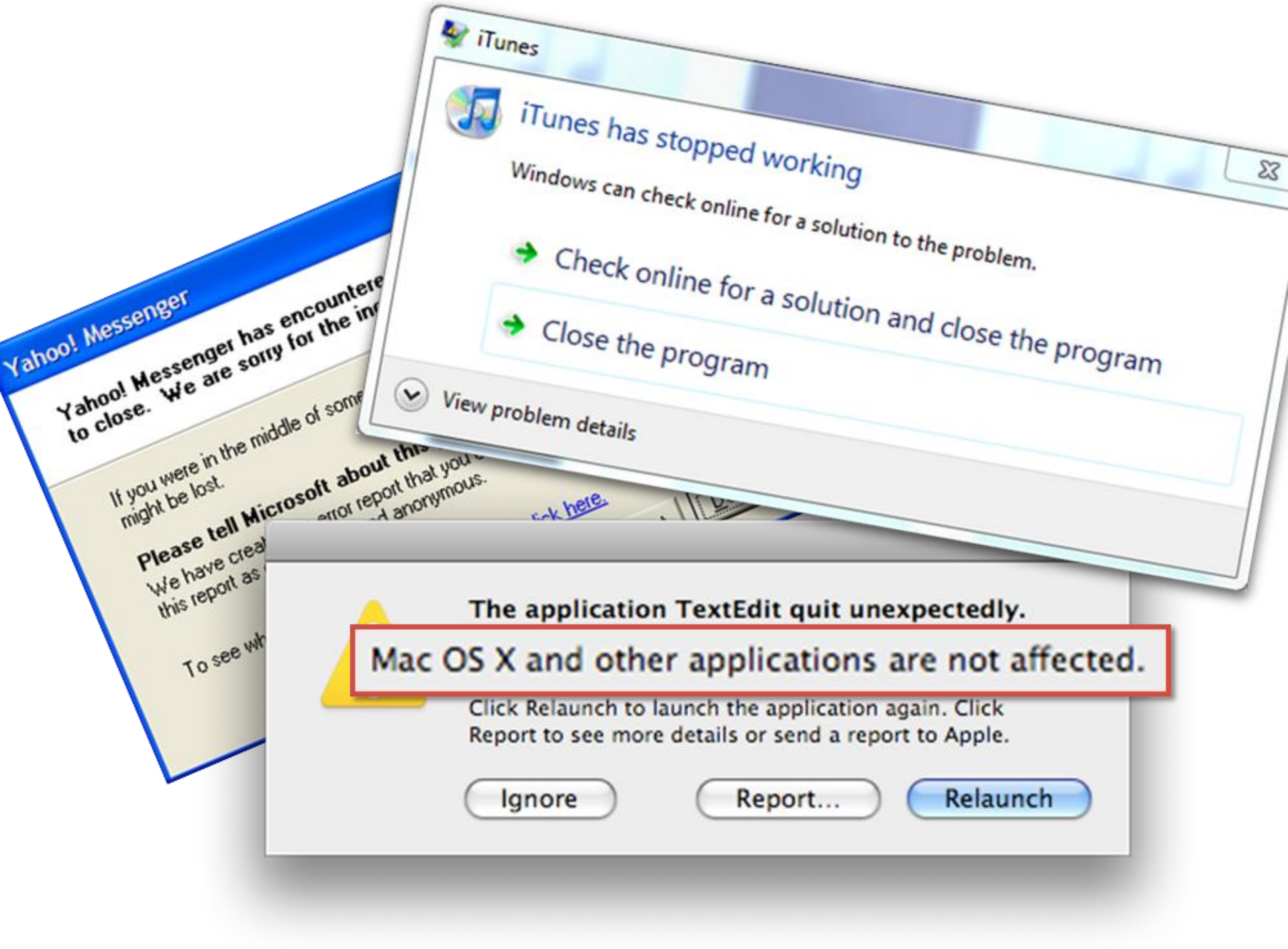
History of Ramsauer-Townsend

- Ramsauer (1921) discovers unexpected behavior in scattering experiments
- Townsend and Bailey (1922) confirm effect using a different method
- Bohr proposes interference of matter waves
- Effect explained using Schrödinger equation (1927-31)

Pulsed NMR

- Nuclear spins precess around static magnetic field
- Oscillatory perpendicular field $\rightarrow$ nutation
- Perpendicular spin component induces measurable current




Yahoo! Messenger
Yahoo! Messenger has encountere
to close. We are sorry for the in
If you were in the middle of some
might be lost.
Please tell Microsoft about this
We have creat
this report as
anonymous.
To see wh
iTunes
iTunes has stopped working
Windows can check online for a solution to the problem.
Check online for a solution and close the program
Close the program
View problem details
The application TextEdit quit unexpectedly.
Mac OS X and other applications are not affected.
Click Relaunch to launch the application again. Click
Report to see more details or send a report to Apple.
Ignore
Report...
Relaunch

Ideas from the classification of cycle structure, cont

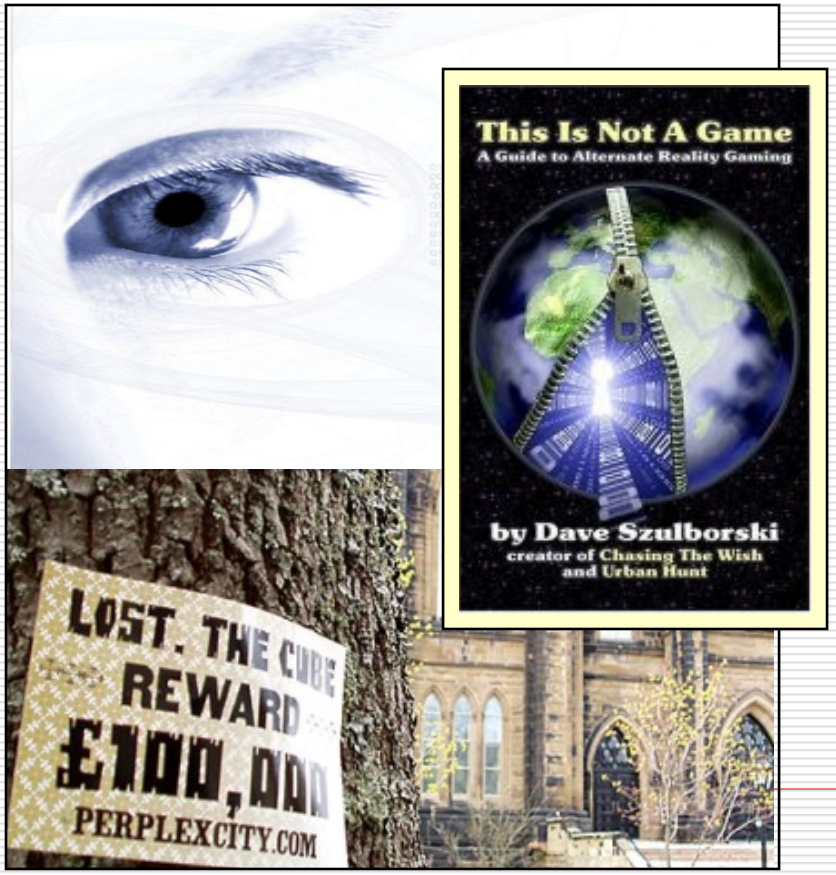
To show that each residue class contains exactly one residue class, we note that if x is in a cycle of length j, then

$$\sigma_{abc}^{j}(x) = x + m(a+b) - ld = x.$$

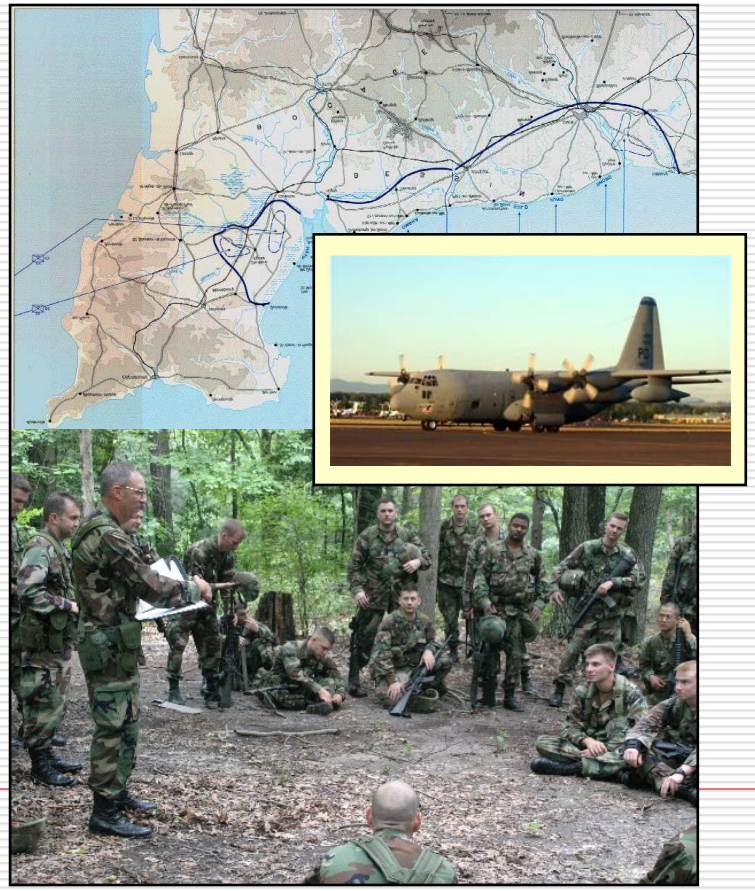
and $m + l \leq j$.
We show that $\lceil \frac{n}{k} \rceil / 2 < j$.

Inspirations For Helical Training

Alternate Reality Games



Large-scale exercises

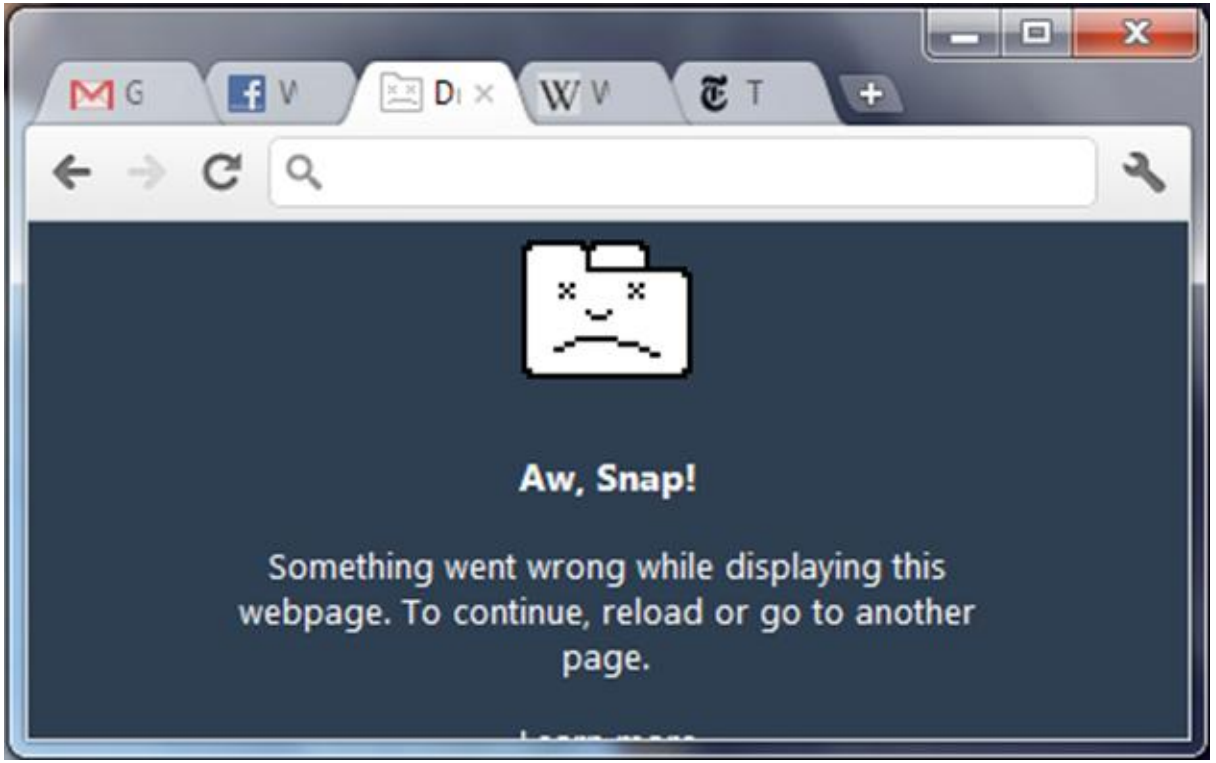


Playing in the sandbox

- How tab isolation works
- Sandboxing
- Principle of least privilege

Tab isolation

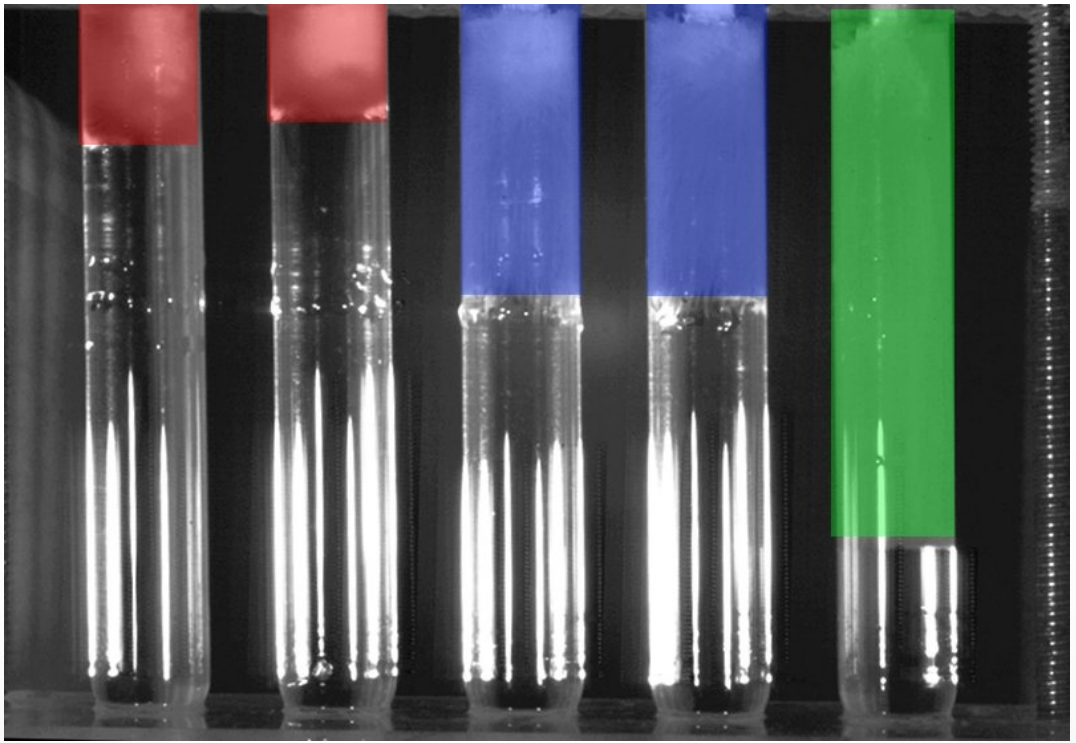
- Chrome brings the same isolation to webpages
- One crashed tab doesn't kill the browser



Multi-process browsing

- Each tab in a separate renderer process
- Renderers coordinated by browser process
- Communicate by sending messages
- Renderer bugs are recoverable
  - Browser process crashes are still fatal

High Speed Crystallization of Sodium Acetate



Robin Deits, **Sally Wolfe**, Daniel Ron, Bayo Olatunji

Questions?

- History of Compton Scattering
- Scattering Theory
- Amplitude Experiment
- Attenuation Experiment

Idea of the construction of $\mathbf{p}_k(n)$, cont

Then

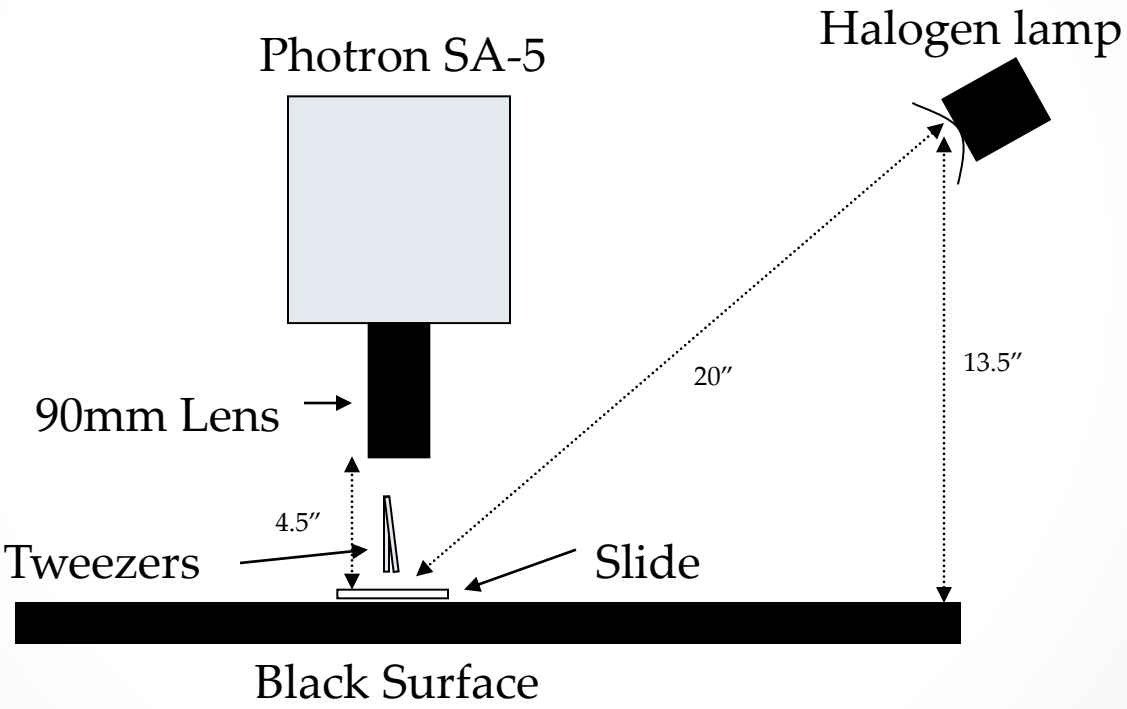
$$\mathbf{p}_k(n) = f(n,k) \cdot Pr(B_k \text{ given } A_k).$$

If $n \mid k$, we have that $k \mid (a+b)$ and $(b+c)$ implies that $k \mid a, b, c$. Then choosing the blocks a, b, c partitioning n is equivalent to choosing blocks $a/k, b/k, c/k$ partitioning n/k.

Then $Pr(B_k \text{ given } A_k) = \mathbf{p}(n/k)$, so

$$\mathbf{p}_k(n) = f(n,k)\mathbf{p}(n/k).$$

Procedure: overhead setup



Limit of $\mathbf{p}_k(n)$

Theorem

We have

$$\lim_{n\to\infty} \mathbf{p}_k(n) = \frac{1}{k^2}\frac{6}{\pi^2}.$$

This is actually useful!

Applications

- Polymer formation
- Cell behavior
- Statistical mechanics
- Financial modeling
- Societal evolution
- Data compression
- Music

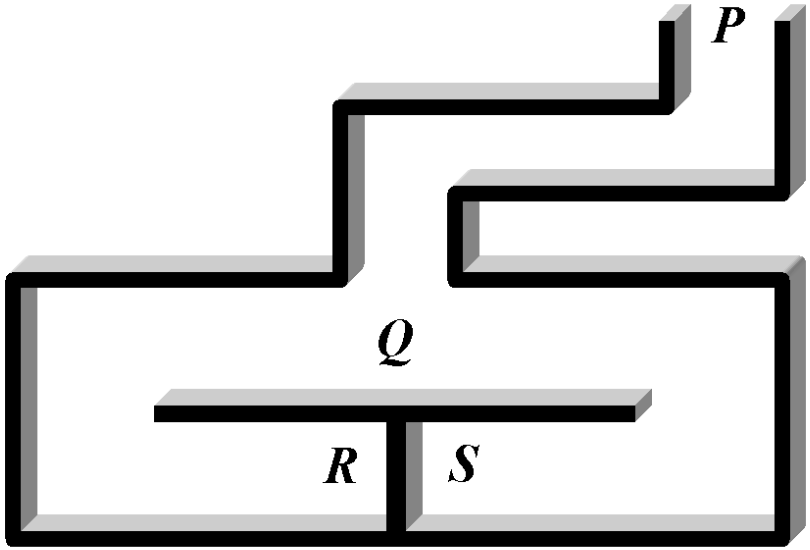
Hidden Markov models

- Cryptography
- Error correction
- Speech recognition
- Computer vision
- Machine translation
- Fraud detection
- Pattern recognition

Prior Art: Custom rules

- Hand-written to match whatever the server in question is doing
- "Only allow the web server to access files under /var/www/"
- "Only allow the ssh server binary to bind to port 22"

Problem: Ali Baba's Cave



- Imagine that you (Peggy) are exploring a cave with a friend
- You know a secret password to get through the door between R and S
- You want to prove to your friend Victor that you know the password, without him finding out the password.

Image: RSA Laboratories

Playing in the sandbox

- All complex software is buggy, so design for bugs
- Separate renderer process per tab
  - Improved stability
  - Security
- Restrict renderer rights to bare minimum
- Principle of least privilege
- Questions?

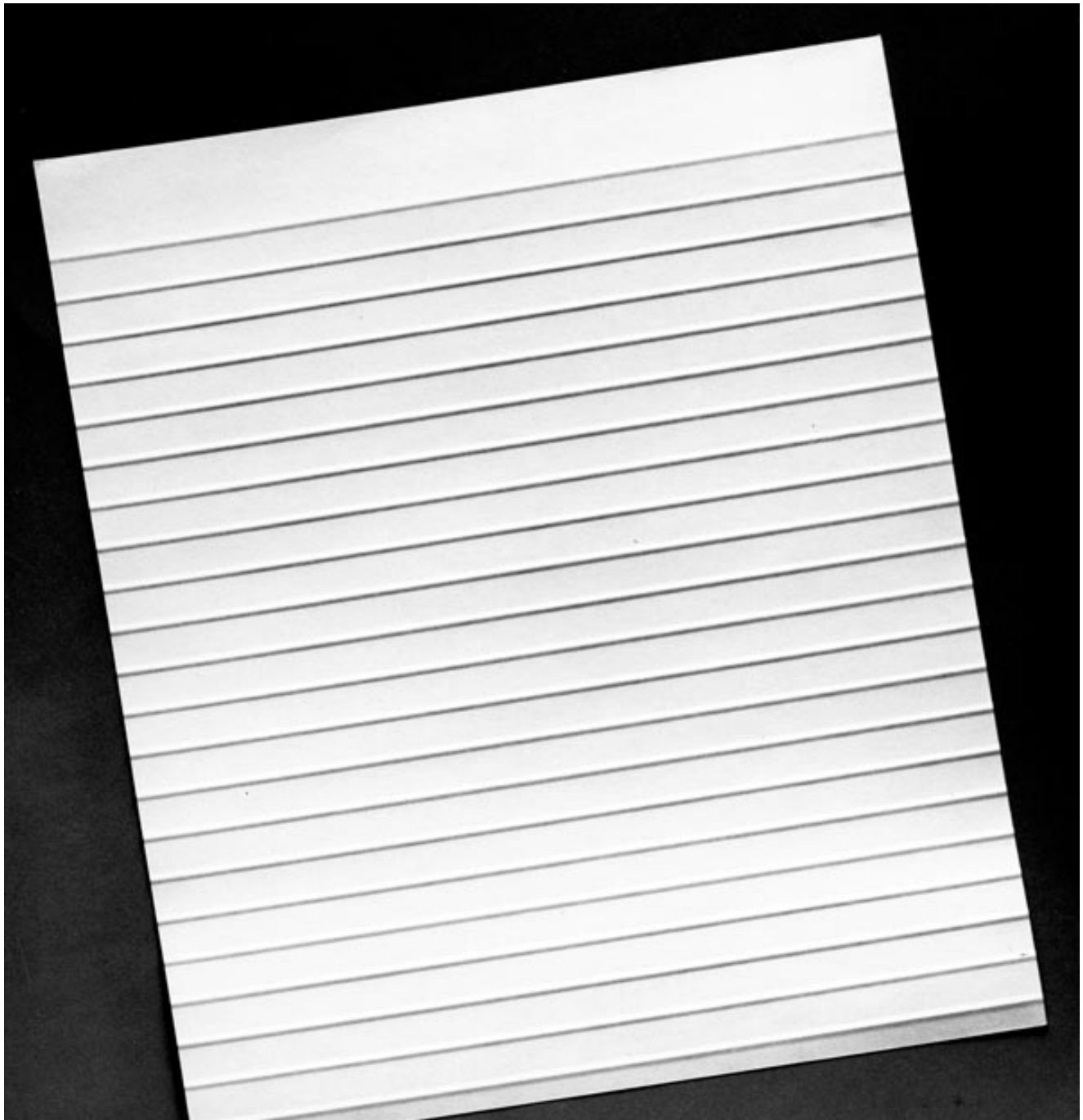
Problem

- Security is a growing issue
- Huge amounts of money are being spent, both to defend against attacks and to clean up after them
- Host-based intrusion detection systems monitor servers to detect attacks
- Security software is sometimes specifically targeted

Choosing behavior based on error

- Desired result
- Method of making error measurement
- Way to control the system
- Way of deciding what to do based on error

Paper



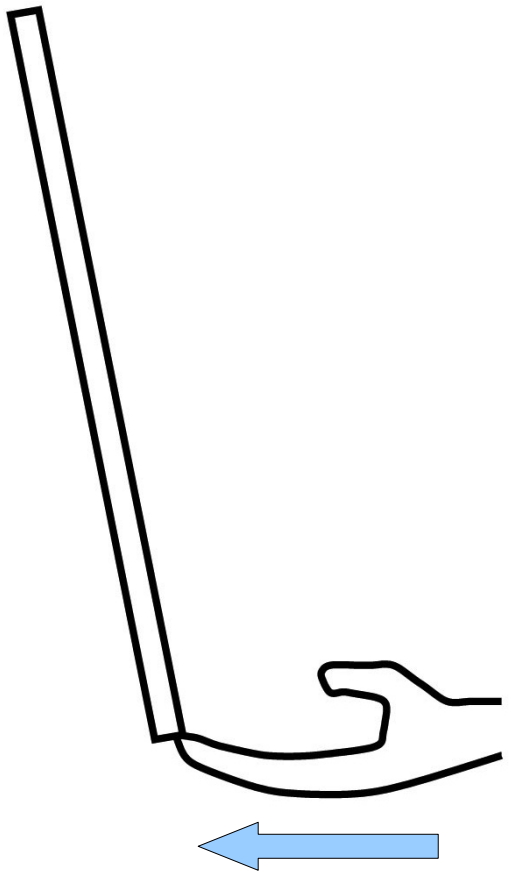
How to Sound Like a Human

(by forgetting your past)

Alan Huang

Fistful of Dollars (RPP)

Unstable systems



History of a phenomenon

Discovery

- Hertz's radio experiments (1886-7)
- Ultraviolet light and electricity

Investigation

- Lenard's experiment (1902)
- Energies independent of intensity
- But dependent on frequency!

Understanding

- Einstein's explanation (1905)
- Light quanta with $E \propto \nu$
- Millikan's experiments (1912-5)

Conclusion

- Security becoming increasingly important
- Host-based intrusion detection vulnerable to the agent being attacked
- Project: *Enhance effectiveness of intrusion detection systems by moving the vulnerable agent onto the host, and use vprobes to look inside the VM*
- Extensive literature exists on how to examine the data the agent/vprobes gather

abc-permutations

Definition

Let *abc*-permutations be elements of S_n obtained by partitioning $[n]$ into three blocks of length a, b, c and exchanging the first and last blocks.

Proof of classification of *abc*-permutations

Assume that σ is reverse layered and avoids 4321. Then it has at most three layers, so it is an *abc*-permutation.

Now assume that σ is an *abc*-permutation. Then it is reverse layered, so it avoids 132, and 213. It also has at most three layers, so it avoids 4321.

Questions?

- History of Ramsauer-Townsend
- Scattering
- Matter Waves
- Dependence of cross section on energy

Results and Errors

- $h = (6.348 \pm 0.0626) \cdot 10^{-34}\ \mathrm{J \cdot s}$
  - $\approx$ 4.2% off of true value ($\approx$ 4.5 times estimated error)
- $\phi = 1.76 \pm 0.026\ \mathrm{eV}$
  - $\approx$ 23% off of true value ($\approx$ 21 times estimated error)

- Random Errors
  - Precision of instruments
  - Small compared to...
- Systematic Errors
  - Ambient light
  - Light striking the anode
  - Cutoff voltage bias
  - Variation of ϕ

- Various possibilities for systematics, but probably not due to measurement error
- Disparity in error makes some possibilities less likely

Single-process browsing

Chrome browser process

Work of Pak and Redlich

In 2008, Pak and Redlich investigated the probability that an *abc*-permutation of length n is a single n-cycle in order to answer a question posed by V. I. Arnold.

Theorem (Pak-Redlich, 2008)

Let σ_{abc} be an abc-permutation. Then σ_{abc} is a long cycle if and only if

$$\gcd(a+b, b+c) = 1.$$

Background: crystallization

- Crystallization refers to the formation of solid crystals from a homogeneous solution.
- It is essentially a solid-liquid separation technique and a very important one at that.
- Solubility - Hot liquid dissolves more compounds. Once cooling process starts, compounds become crystals

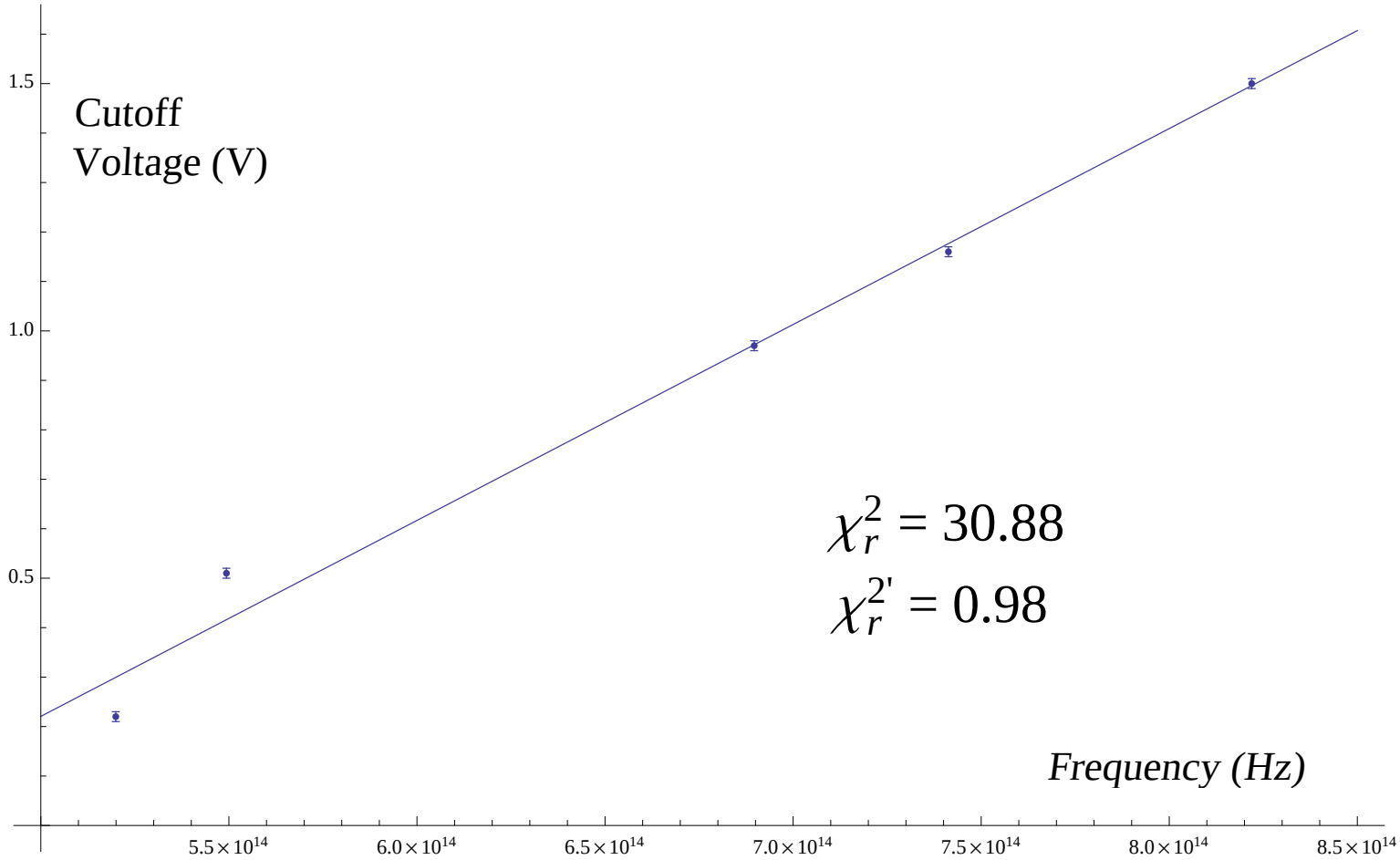
Cycle structure of *abc*-permutations

We fully characterize the cycle structure of *abc*-permutations.

Theorem

Let $k = \gcd(a+b, b+c)$. *Then* σ_{abc} *is composed of* k *cycles of lengths* $\lfloor \frac{n}{k} \rfloor$ *and* $\lceil \frac{n}{k} \rceil$. *These cycles correspond to the residue classes of* n *modulo* k.

Cutoff Voltage vs. Frequency



- Large χ^2 for small ν
- However, near-linear relationship as expected

Ideas from the classification of cycle structure, cont

Therefore, for all i and x we have

$$\sigma_{abc}^{i}(x) = x + m(a+b) - ld.$$

for some integers m, l satisfying $|m| + |l| \leq i$.

Let $k = \gcd(a+b, d) = \gcd(a+b, b+c)$. Then the orbit of x under σ_{abc} will stay within one residue class modulo k.

Questions
?

Using VProbes for Intrusion Detection

Alex Dehnert

VMware Intern, Summer 2011
Massachussetts Institute of Technology, S.B. 2012

Thursday, September 15, 2011

Work of Pak and Redlich

In 2008, Pak and Redlich investigated the probability that an *abc*-permutation of length n is a single n-cycle in order to answer a question posed by V. I. Arnold.

Cycle structure statistics of *abc*-permutations

We investigate the probability $\mathbf{p}_k(n)$ that a random *abc*-permutation of length n has exactly k cycles.

Theorem

We have

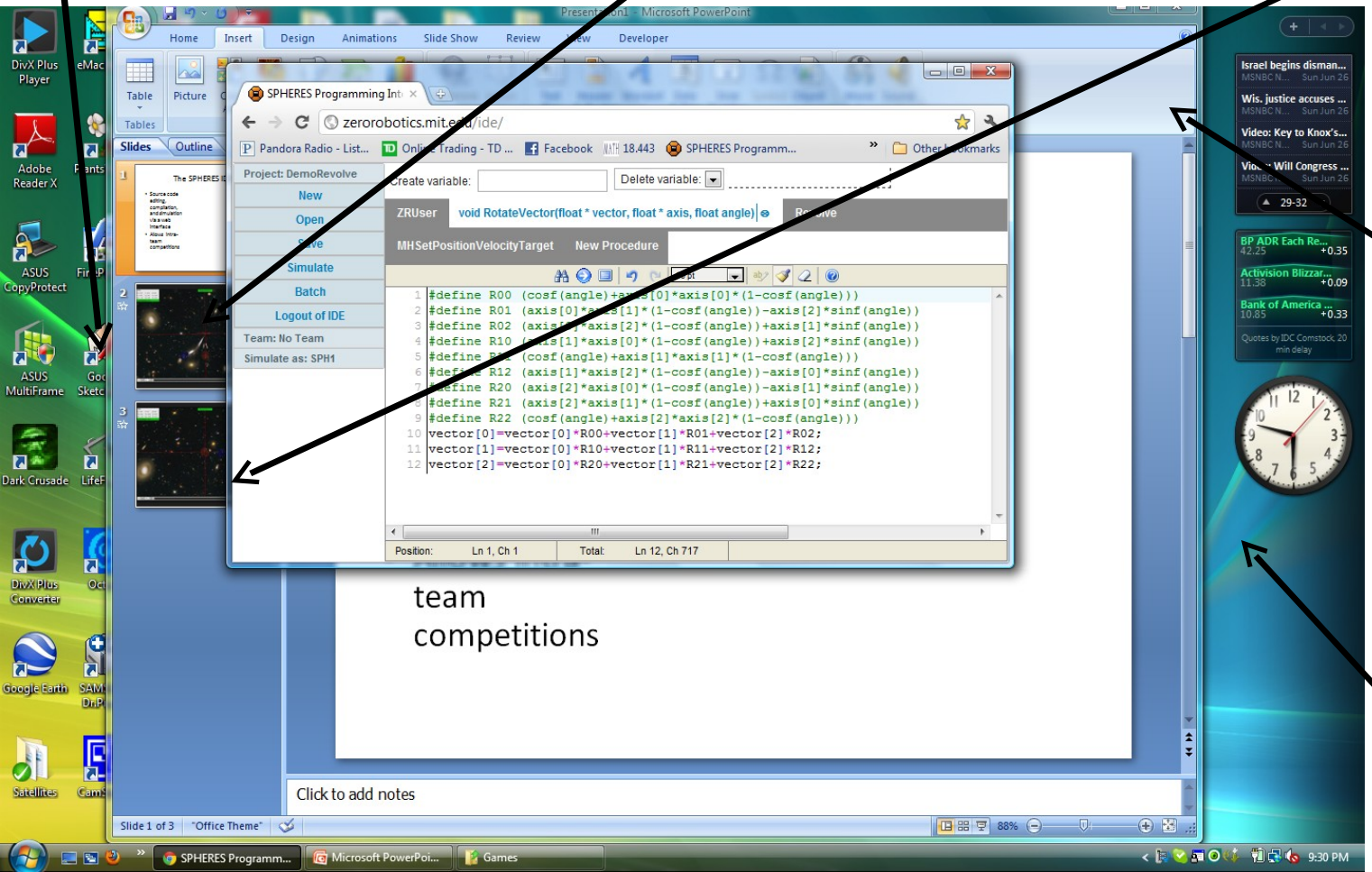
$$\lim_{n\to\infty} \mathbf{p}_k(n) = \frac{1}{k^2}\frac{6}{\pi^2}.$$

The SPHERES IDE

Simulate flight aboard the ISS

Automatic Version Control

Compete with other teams



Web-based

Write and compile C-code

Discussion: summary

Sodium Acetate:

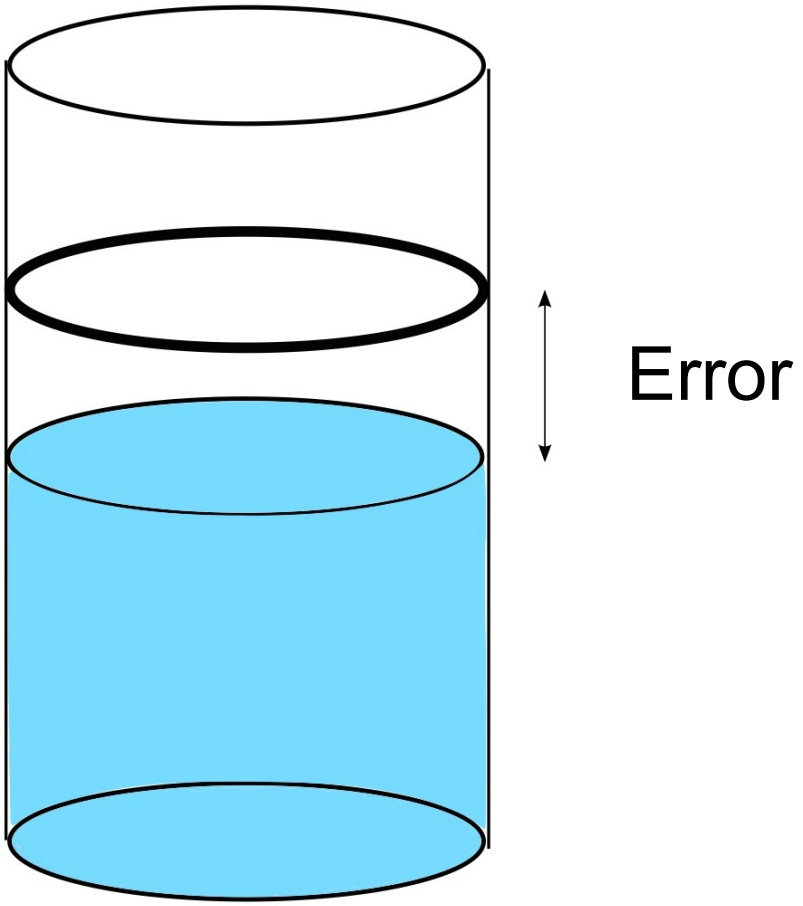
- Crystals form radially outward from seed
- Crystals are long and skinny prisms
- Crystal formation pattern depends on how crystallization is triggered

Bismuth:

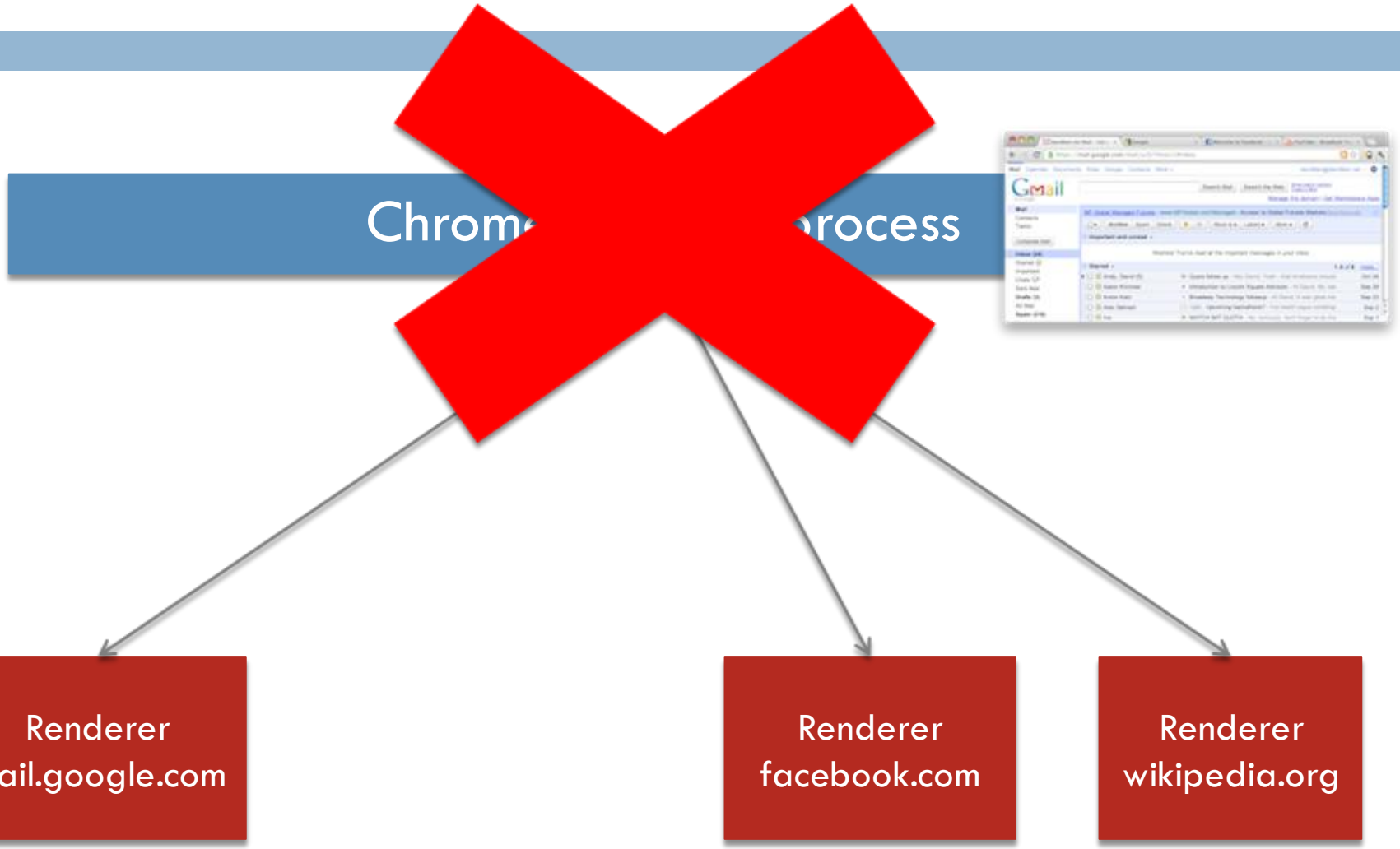
- Difficult to form nice looking bismuth crystals
- Colors won't show up on monochrome high-speed
- No crystal forming process static enough to record

Avalanche (RRR)

Filling a glass to a specific height

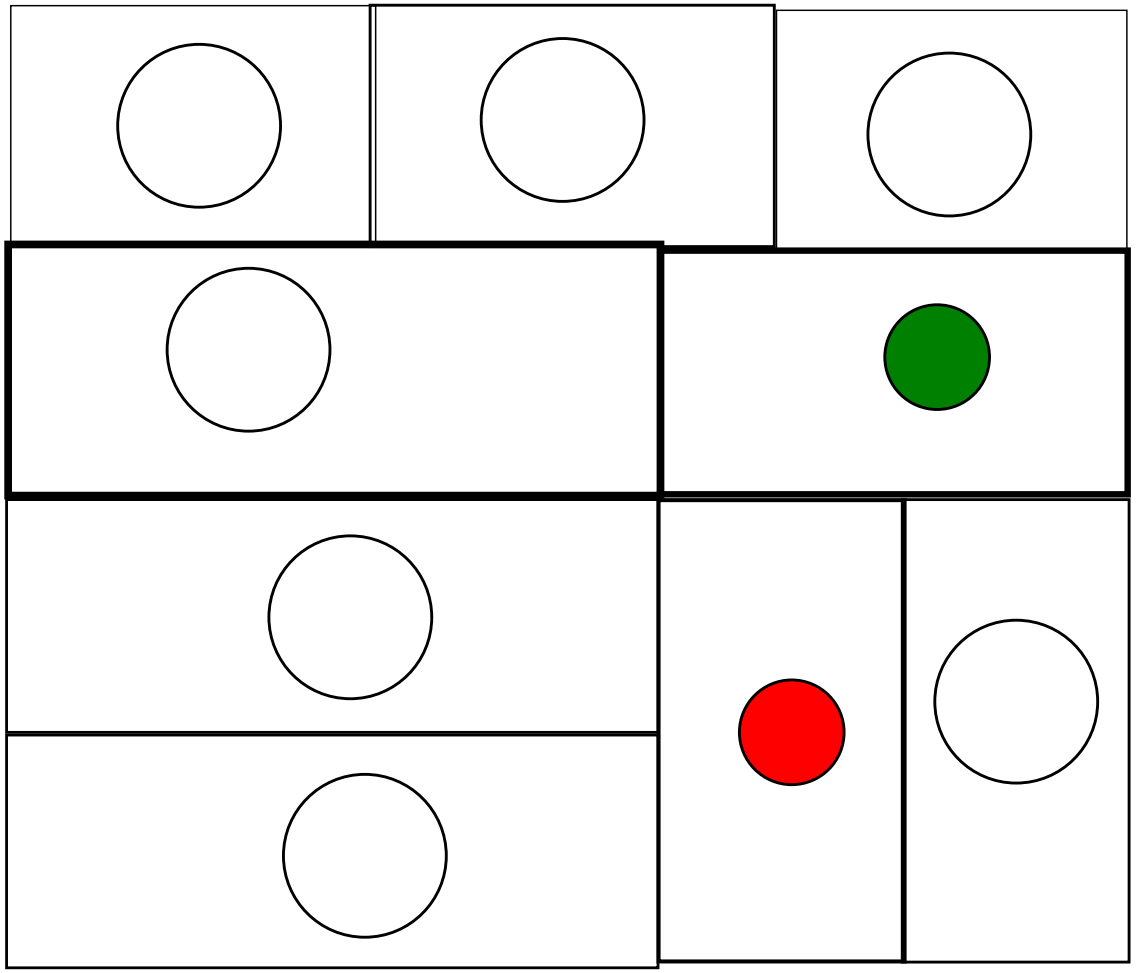


Multi-process browsing



Map coloring ZKP

Respond



Idea of the construction of $\mathbf{p}_k(n)$, cont

Then

$$\mathbf{p}_k(n) = f(n,k) \cdot Pr(B_k \text{ given } A_k).$$

Risks

Big risk: schedule slippage Room to cut in both the exploit finding/writing and the analyzers

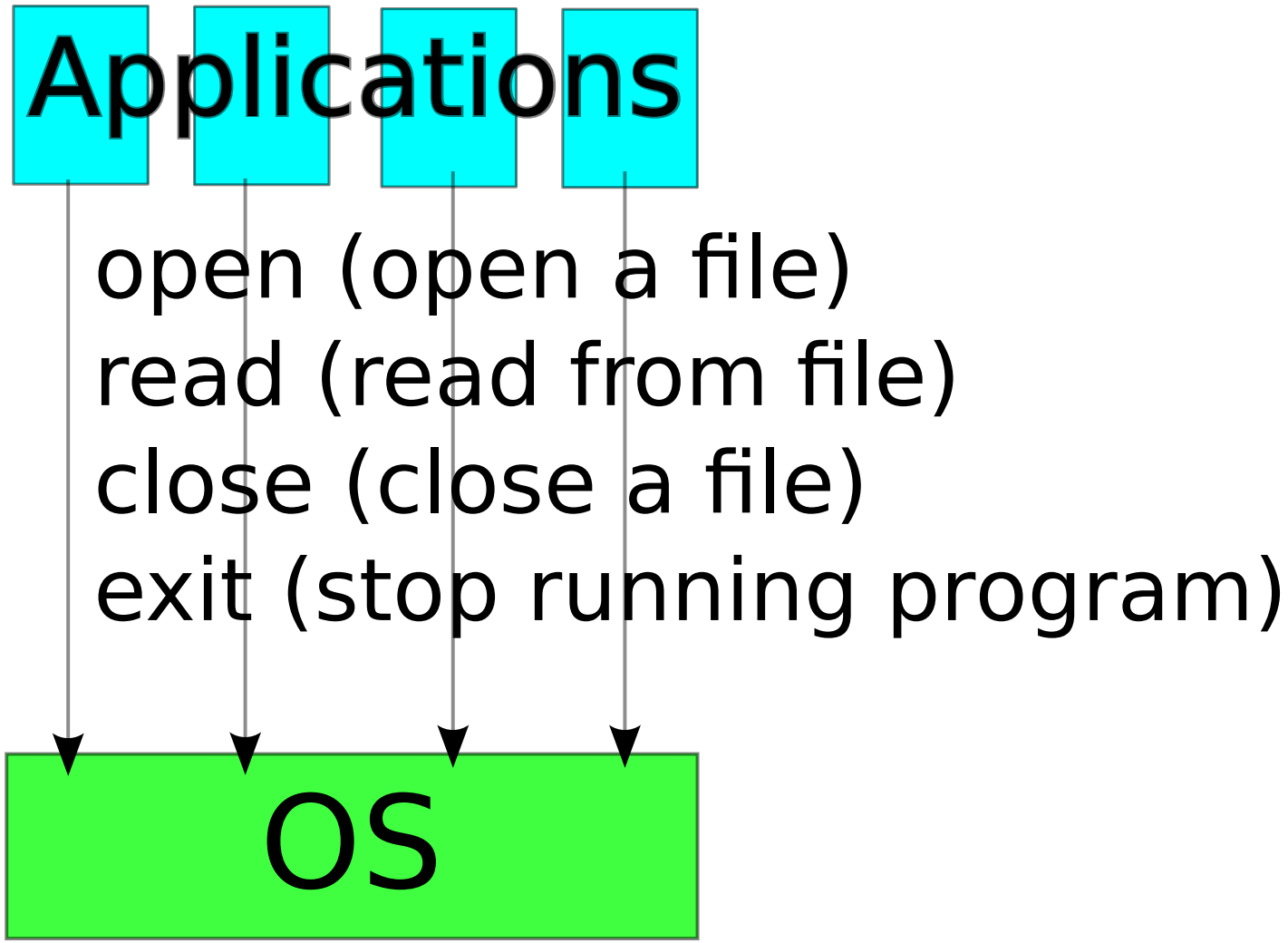
Can't come up with a novel analyzer Not key to the project. The main novelty is supposed to be in the vprobes component, anyway.

vprobes not powerful enough My team is the vprobes team. We can probably add required features.

Enforcing security

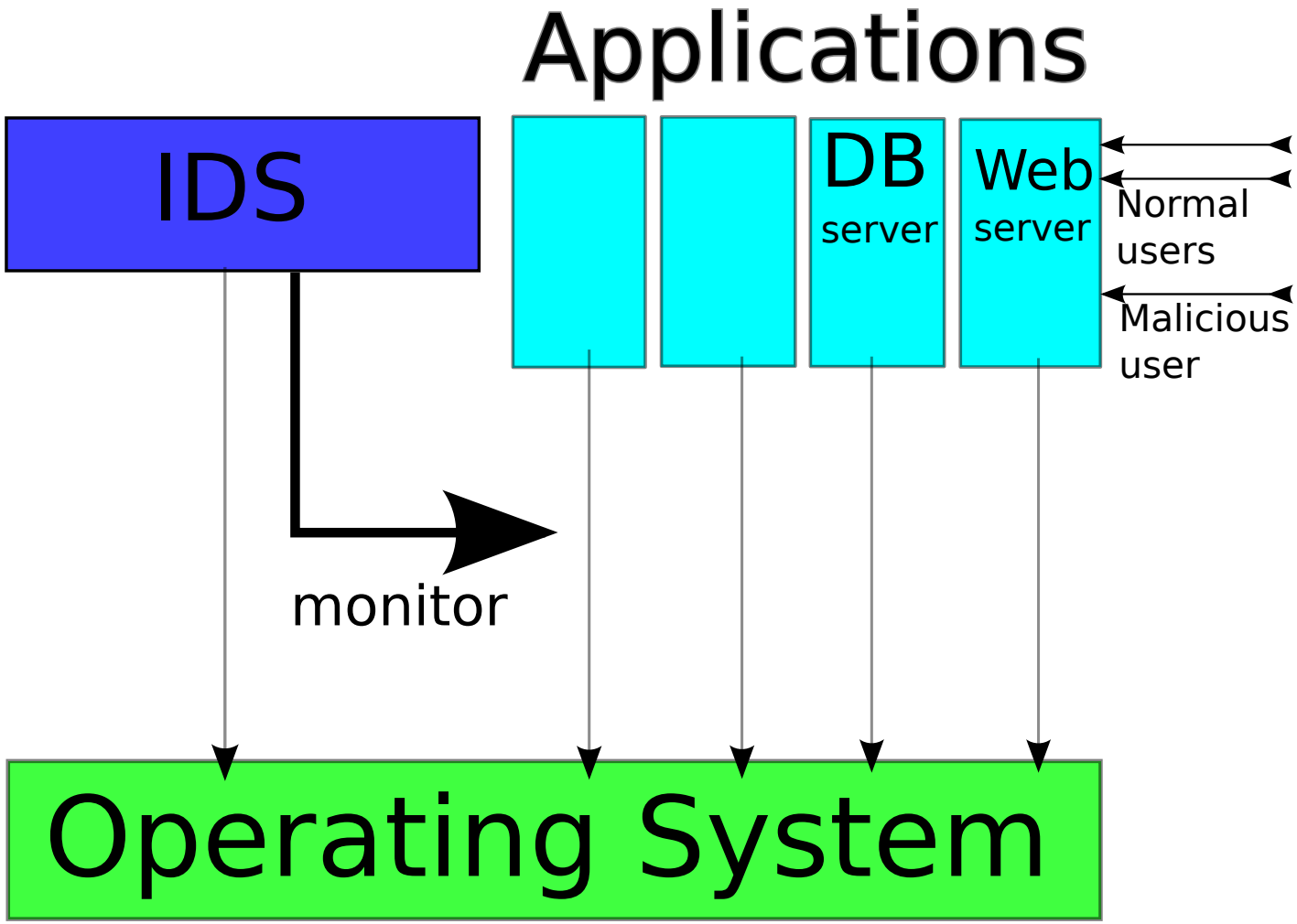
- Sandbox each renderer
  - Can't access files
  - Internet
  - Other processes
- Only communicate with browser
  - Performs privileged actions on behalf of renderer
  - Including network access

System calls (syscalls)



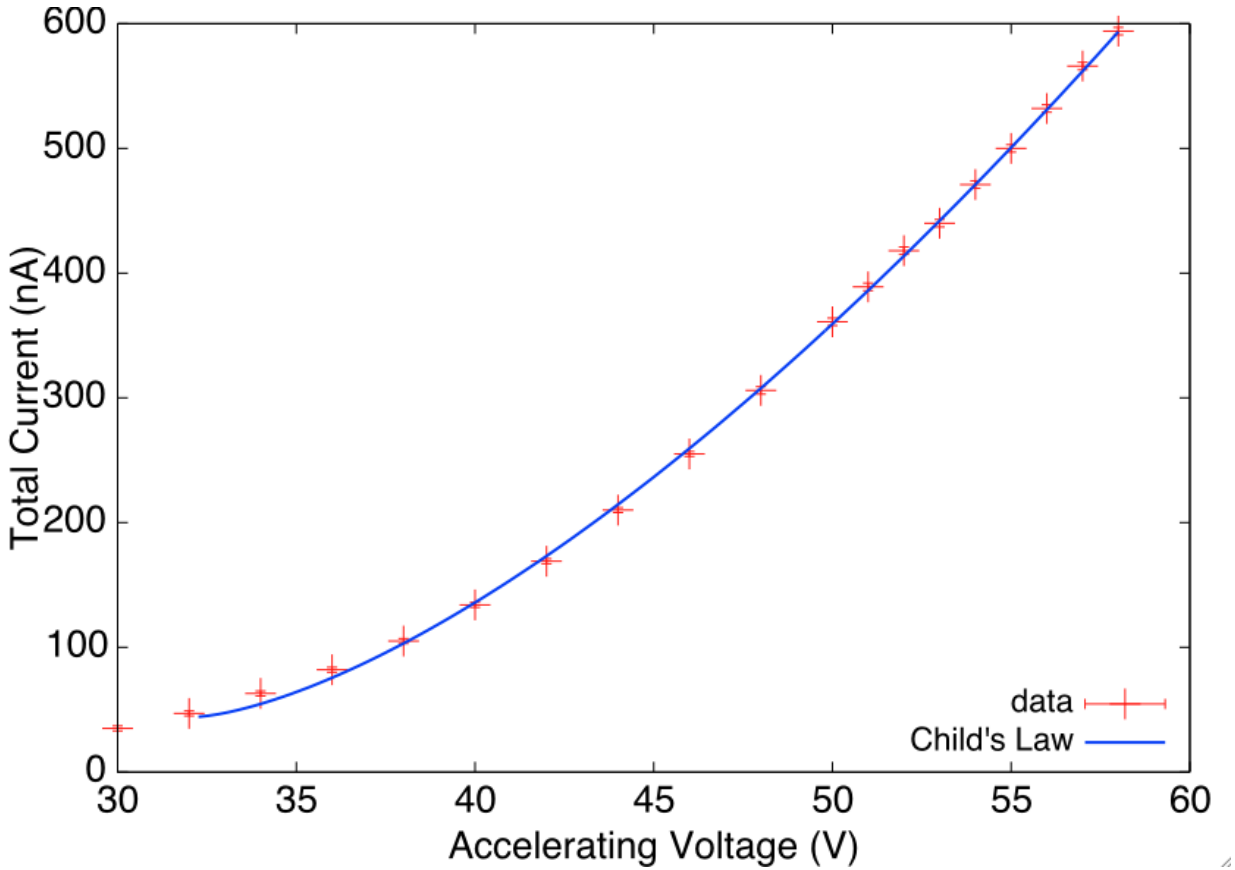
Intrusion detection

- Rich variety of work involving host-based intrusion detection
- Many based on patterns of system calls



Child's Law

- $I \propto V^{\frac{3}{2}}$



$$\chi_r^2 = 4.59$$

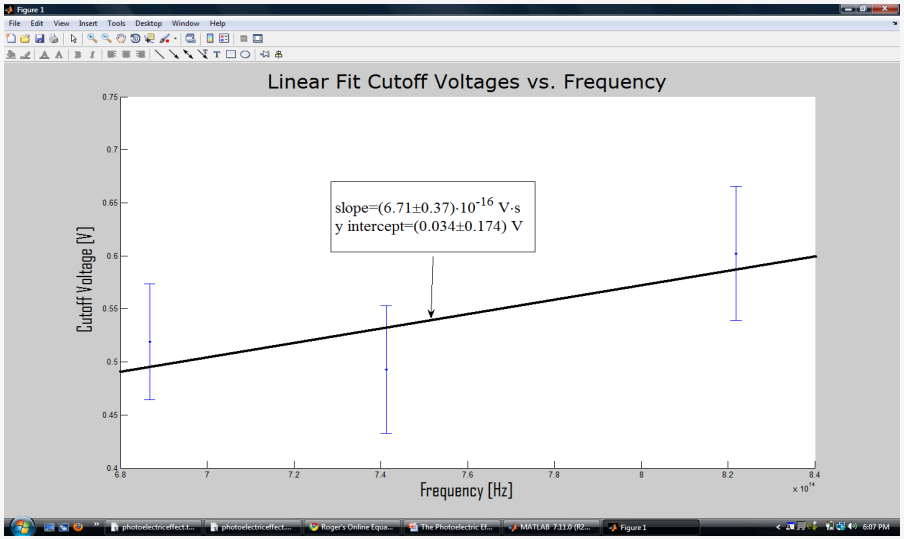
Results

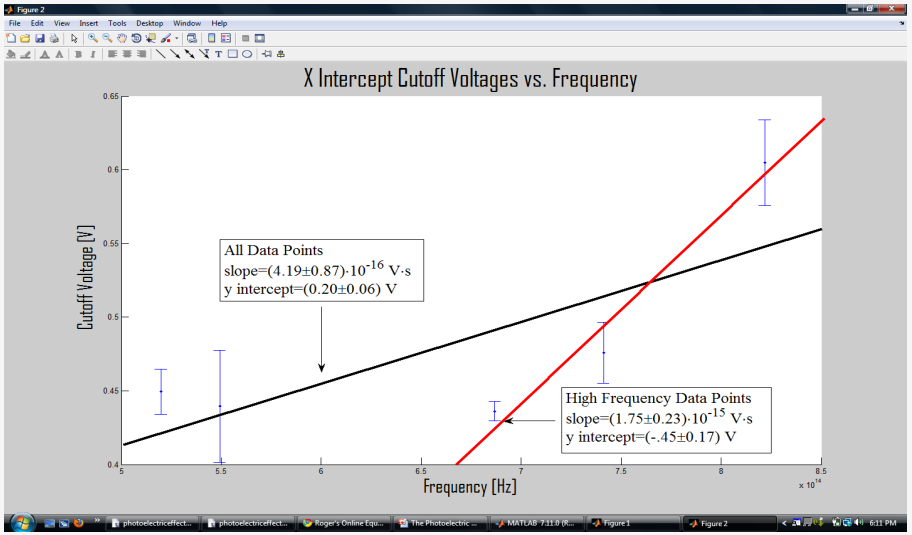
Solidified bismuth drop. Drop was melted in a spoon then poured onto a slide. The line across the middle of the image is the edge of the slide that the drop landed on. Many colors are visible along the various surfaces. f/36, 90mm lens.

Improvements and Extensions

- Additional experiments to determine contact potential and initial electron energy
- Collect more data in vicinity of minimum σ
- Determine voltage necessary to get equal filament temperatures

Graphical Results





Work of Pak and Redlich

In 2008, Pak and Redlich investigated the probability that an *abc*-permutation of length n is a single n-cycle in order to answer a question posed by V. I. Arnold.

Theorem (Pak-Redlich, 2008)

Let σ_{abc} be an abc-permutation. Then σ_{abc} is a long cycle if and only if

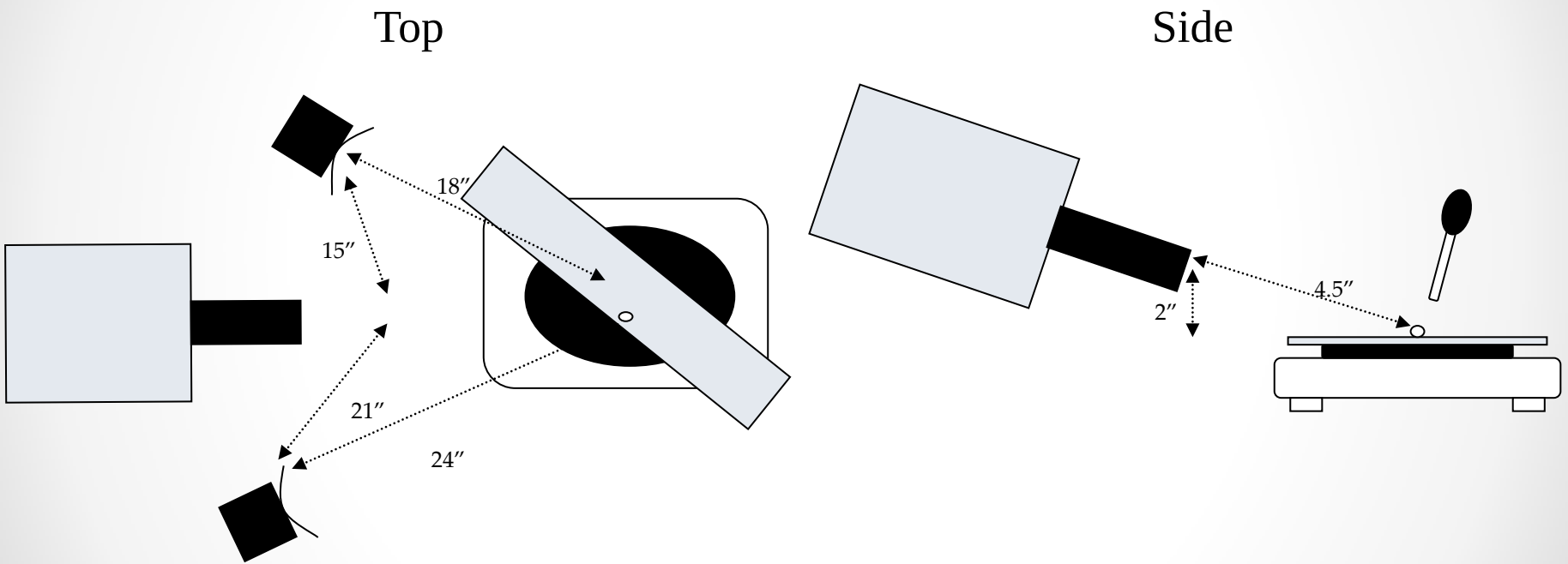
$$\gcd(a+b, b+c) = 1.$$

Theorem (Pak-Redlich, 2008)

Let $\mathbf{p}(n)$ be the probability that an abc-permutation of length n is a long cycle. Then

$$\lim_{n\to\infty} \mathbf{p}(n) = \frac{6}{\pi^2}.$$

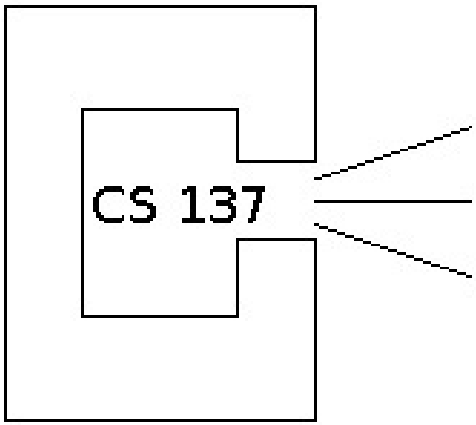
Procedure: boiling setup

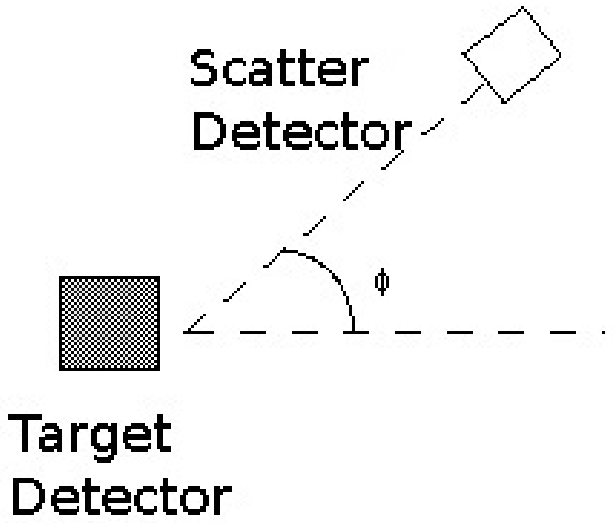


The Photoelectric Effect

Matthew Houston
10/1/2010

Apparatus



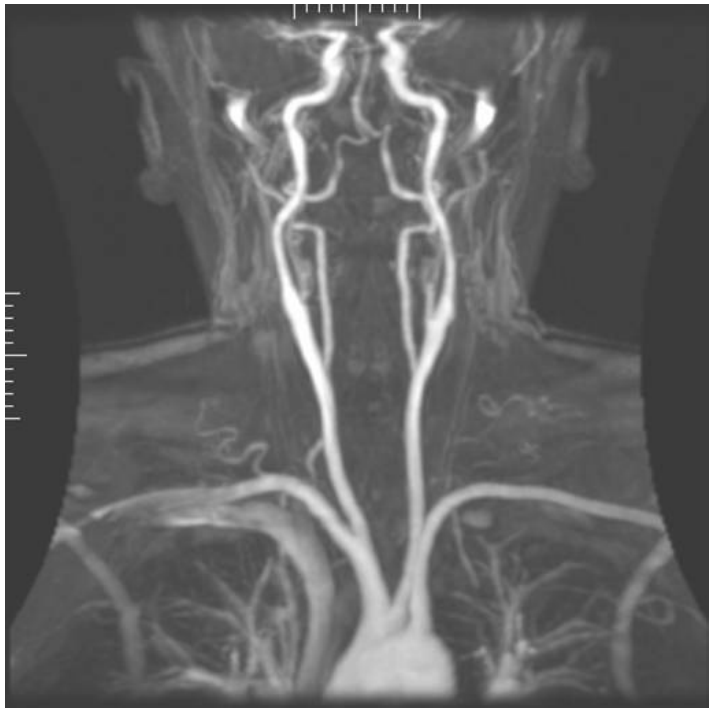


- Discriminators filter out noise
- Coincidence detector selects Compton events

Paramagnetic Ions

- Enormous magnetic moments ($\approx$1000 times proton)
- Much larger interaction energies $\rightarrow$ smaller relaxation times
- Slow local field variations $\rightarrow$ additional T2 mechanism

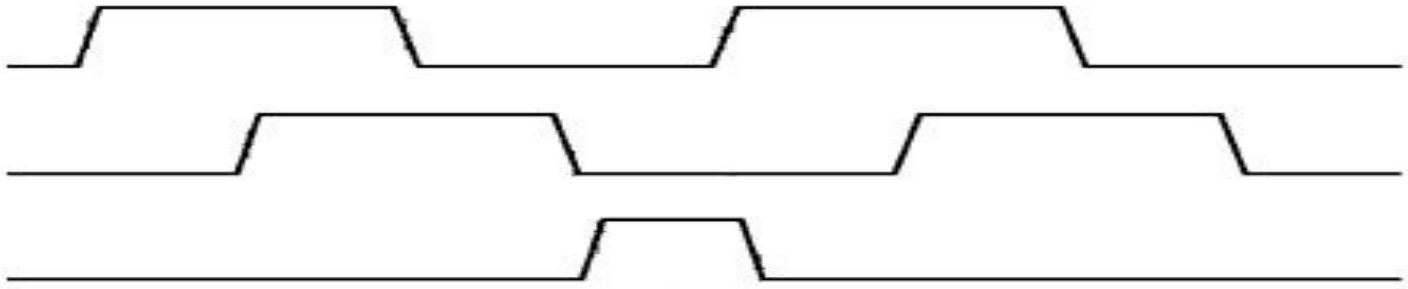
- $\frac{1}{T1} \propto$ ion concentration
- $\frac{1}{T2}$ more strongly affected



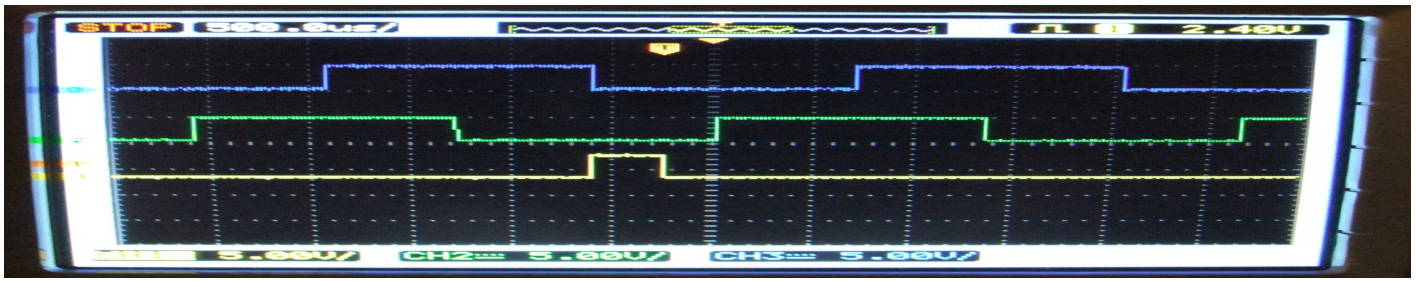
Spinner Assembly: Encoder Testing

Relative roll angle between the bus and payload is given by an optical encoder with 2 arc minute accuracy

US Digital Sample Timing Characteristics



Observed Timing Characteristics



Pattern avoidance and *abc*-permutations

Theorem

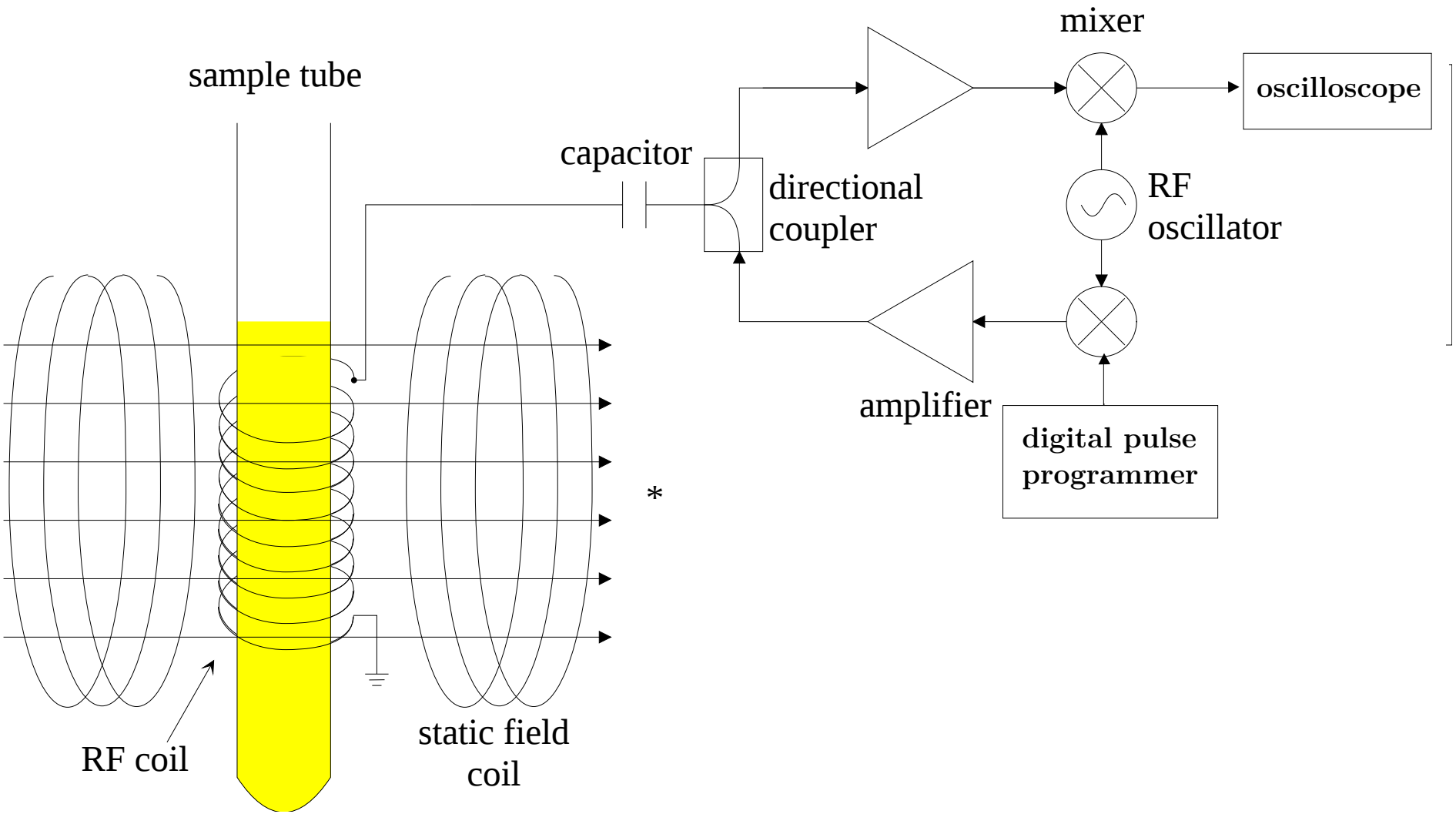
The set of abc-permutations is the set of permutations which avoid 132, 213, *and* 4321.

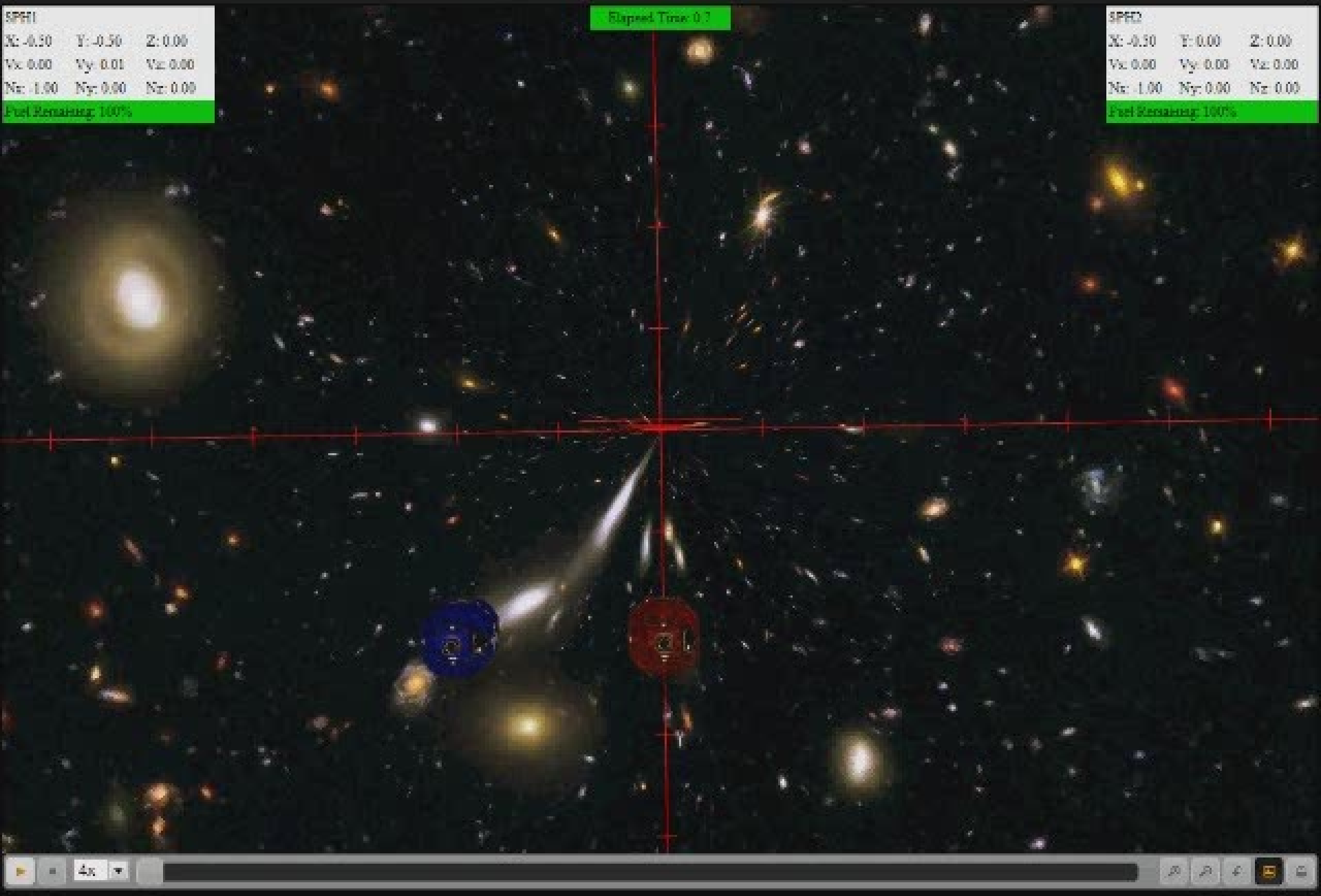
Outline

- Nuclear Magnetic Resonance
- Relaxation and Paramagnetic Ions
- A Useful Tool

Spinner Assembly:

Apparatus


sample tube
capacitor
directional coupler
mixer
oscilloscope
RF oscillator
amplifier
digital pulse programmer
RF coil
static field coil
*


SPH1
X: -0.30 Y: -0.50 Z: 0.00
Vx: 0.00 Vy: 0.01 Vz: 0.00
Nx: -1.00 Ny: 0.00 Nz: 0.00
Fuel Remaining: 100%
Elapsed Time: 0.7
SPH2
X: -0.50 Y: 0.00 Z: 0.00
Vx: 0.00 Vy: 0.00 Vz: 0.00
Nx: -1.00 Ny: 0.00 Nz: 0.00
Fuel Remaining: 100%
4x

General Structure

	Victor stands outside
Peggy: Prepare	Peggy vanishes into the cave
Peggy: Commit	Victor comes back in, . . .
Victor: Challenge	. . . and calls out which side Peggy should return by
Peggy: Respond	

Reverse layered permutations

Definition

A permutation ϕ is called reverse layered if it is of the form $q_1 q_2 \dots q_k$, where the q_i are strings of consecutively increasing numbers and $q_i > q_j$ if $i < j$.

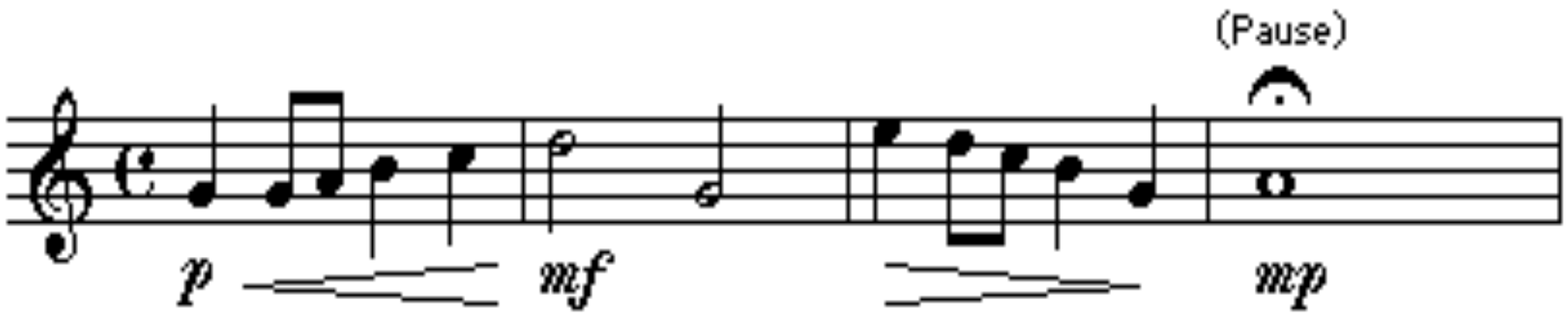
Lemma (Monsour, 2002)

The set of reverse layered permutations is the set of 132 *and* 213 *avoiding permutations.*

Prior Art

Much previous work on how to determine whether or not some sequence of syscalls is allowed

Crescendo (PSR), Decrescendo (RSP)



Bureaucrat (PPP)

Summary

- Observed the Ramsauer-Townsend effect in electron–Xenon collisions
- Found minimum cross-section near expected energy
- Provided evidence for interference in matter waves and quantum theory

Numerical Results

Method	Plank's Constant (Js)	Work Function (eV)
Linear Fit High Freq.	$(1.07 \pm 0.37) \cdot 10^{-34}$	0.03 ± 0.175
X-Intercept High Freq.	$(2.04 \pm 0.37) \cdot 10^{-34}$	-0.45 ± 0.175
X-Intercept All Data	$(6.72 \pm 1.40) \cdot 10^{-35}$	0.20 ± 0.06
Actual	$6.63 \cdot 10^{-34}$	2.3

Experimental results differ from known values by at least an order of magnitude (several standard deviations)

General Structure

Peggy: Prepare

Peggy: Commit

Victor: Challenge

Peggy: Respond

Procedure: underneath setup