Title: What the H&$! is Quantum Information Science?

Date: Jul 29, 2008 09:00 AM

URL: http://pirsa.org/08070044

Abstract:

What the H&$! is Quantum Information Science?

Robin Blume-Kohout

What Information Theory Does

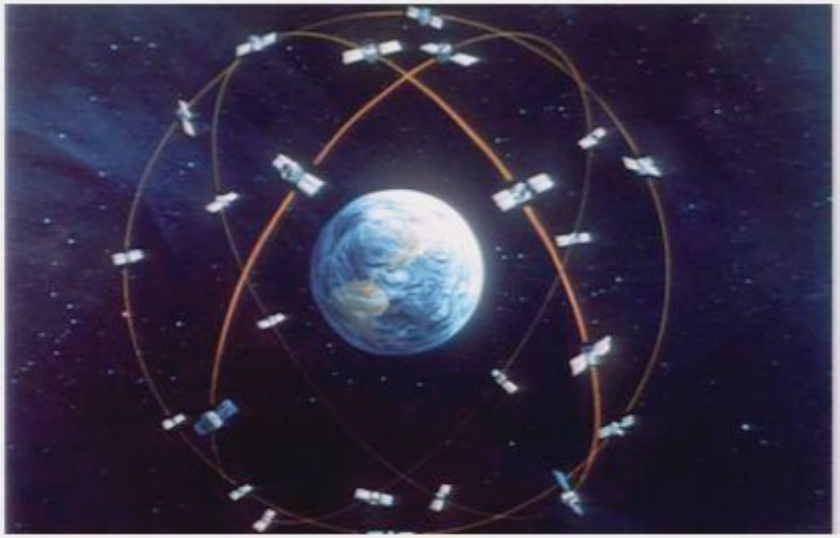
Communication Theory

Communication Theory

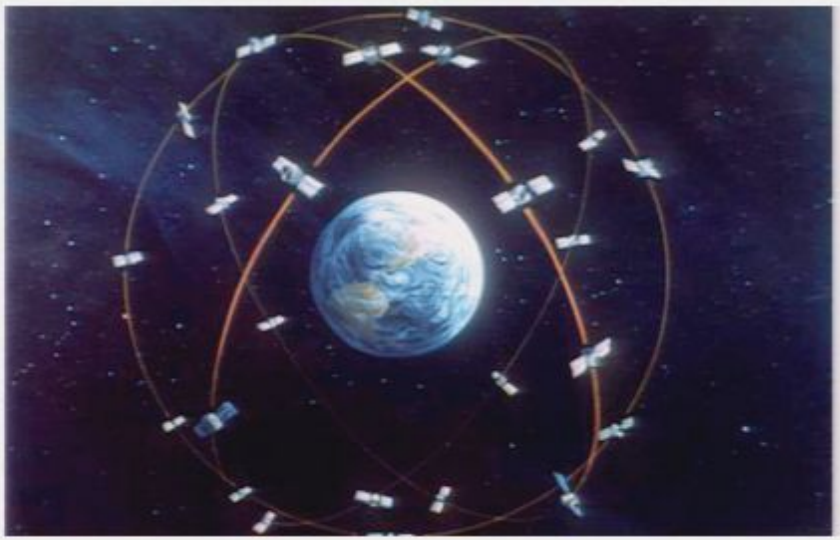
- Lets us lock on to GPS satellites.

Communication Theory

- Lets us lock on to GPS satellites.



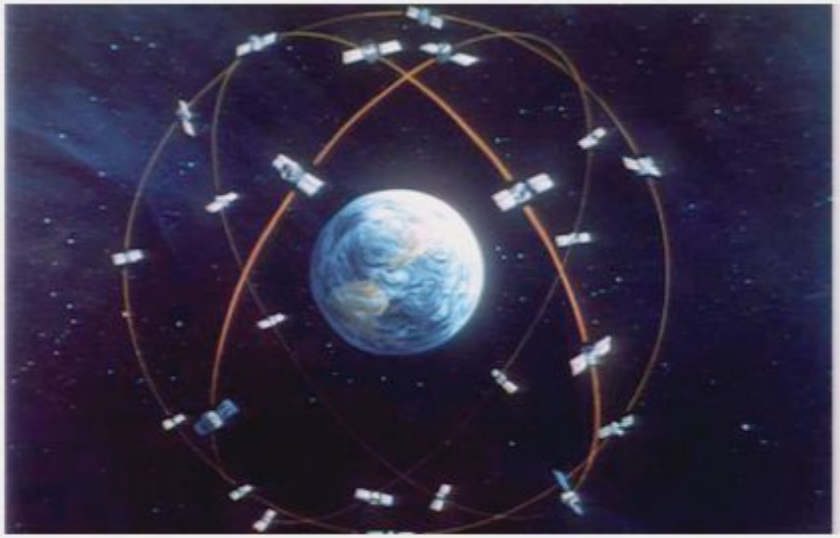
Communication Theory



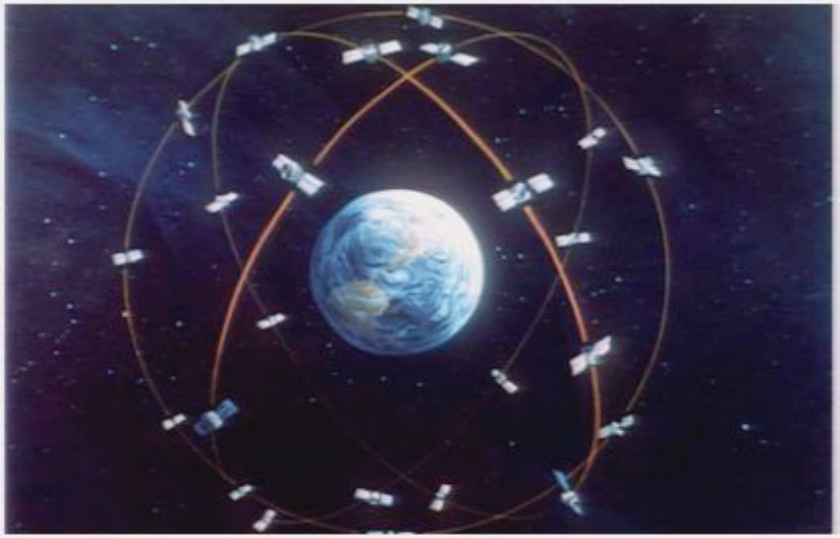
- Lets us lock on to GPS satellites.

Communication Theory

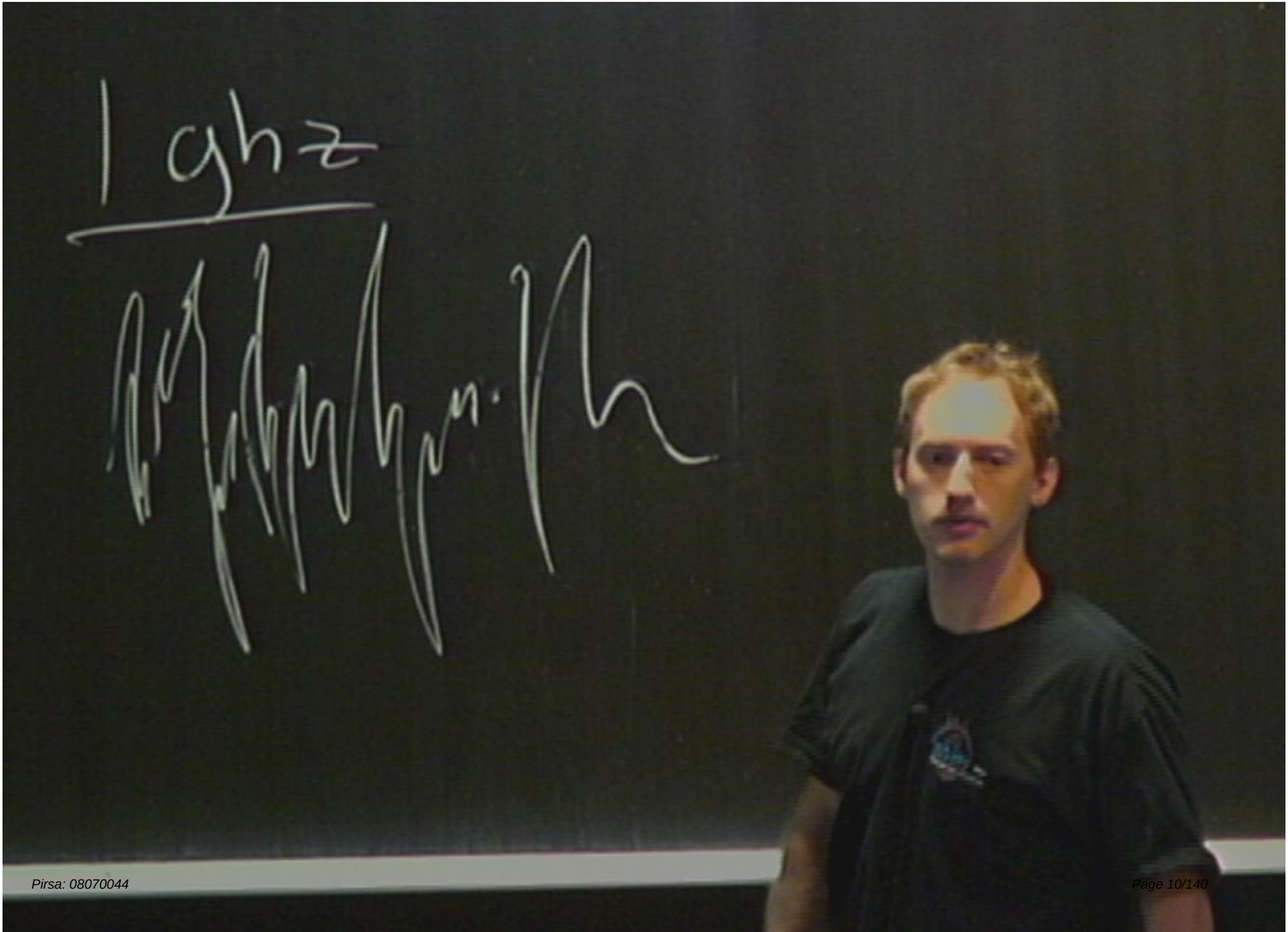
- Lets us lock on to GPS satellites.

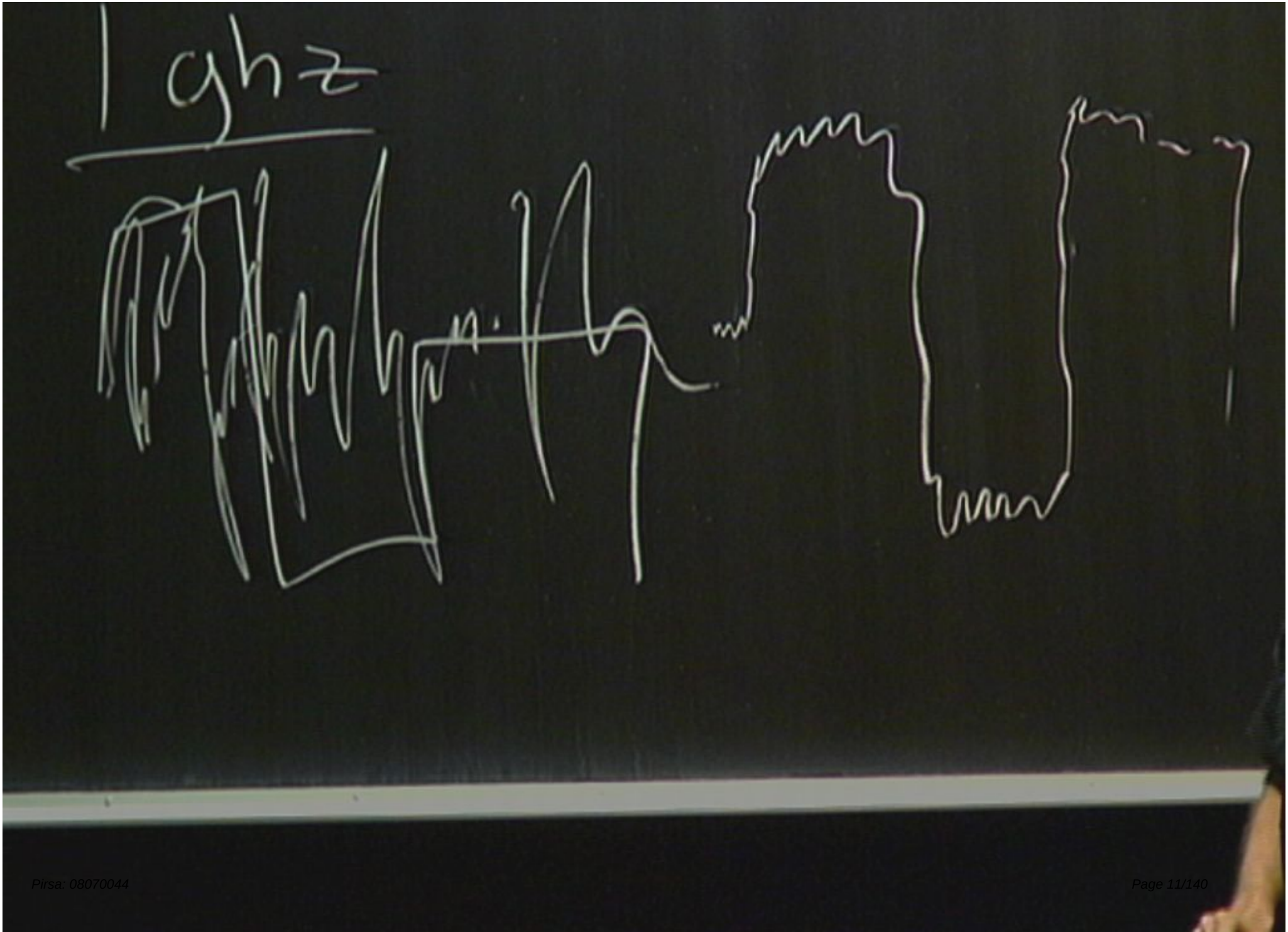


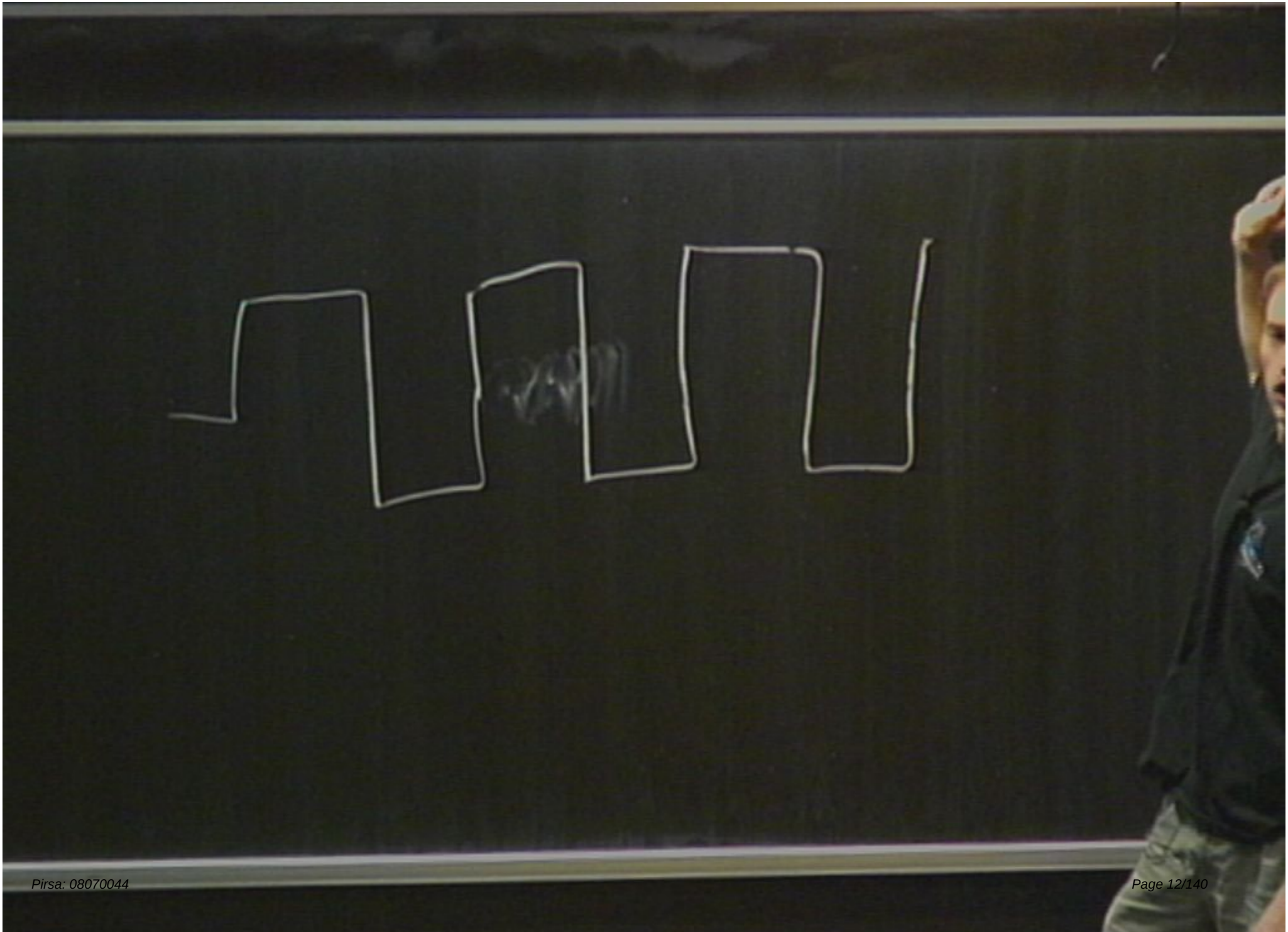
Communication Theory

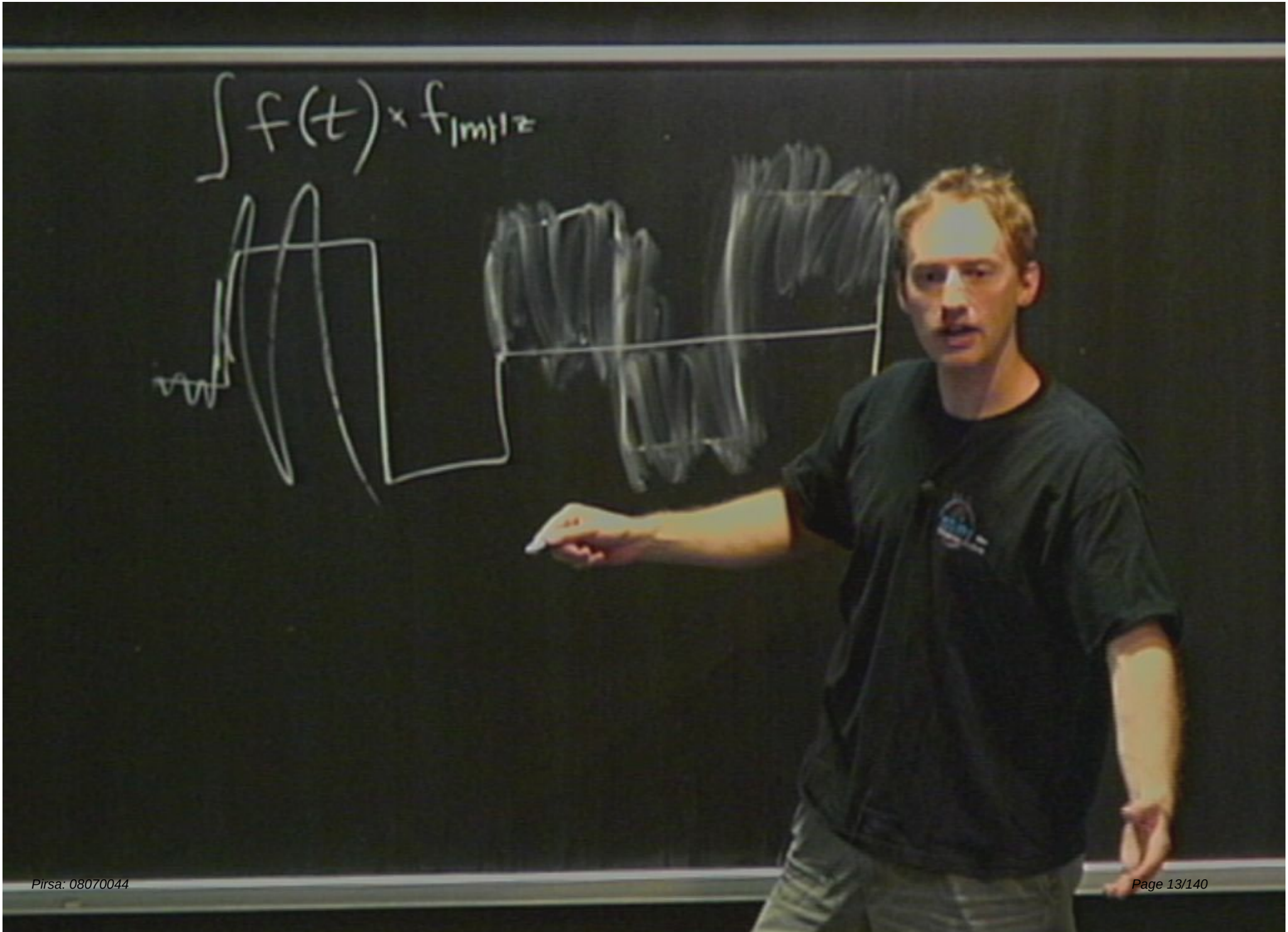


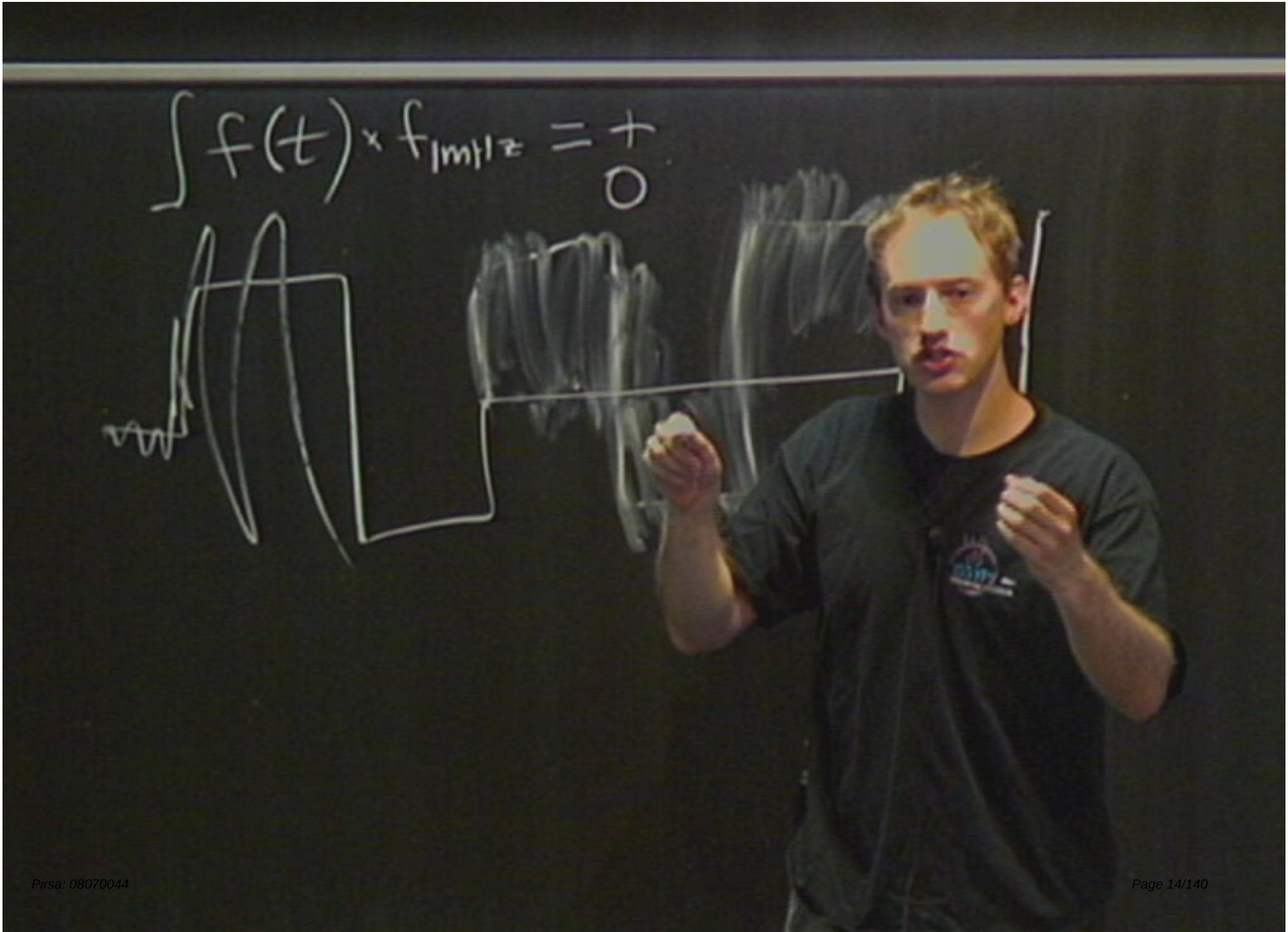
- Lets us lock on to GPS satellites.
- How to communicate despite noise
  - *transmitting information through noisy channels*


1 ghz

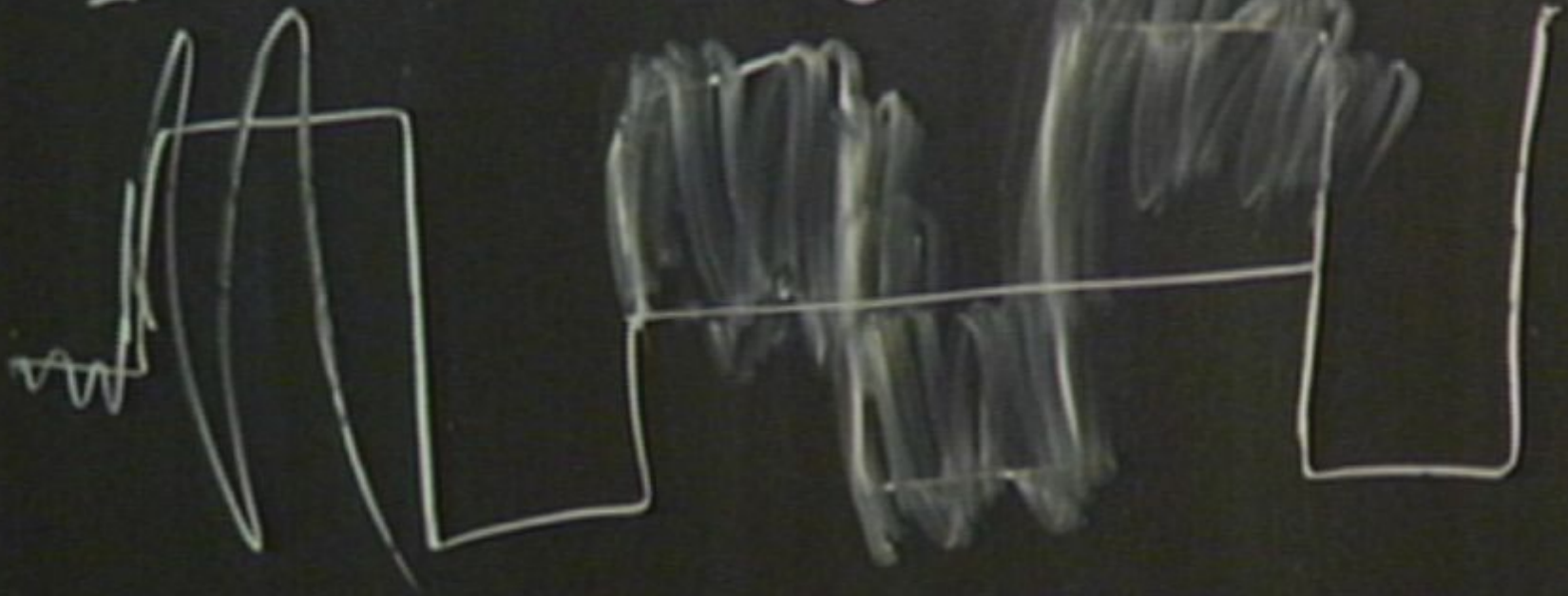

1 ghz



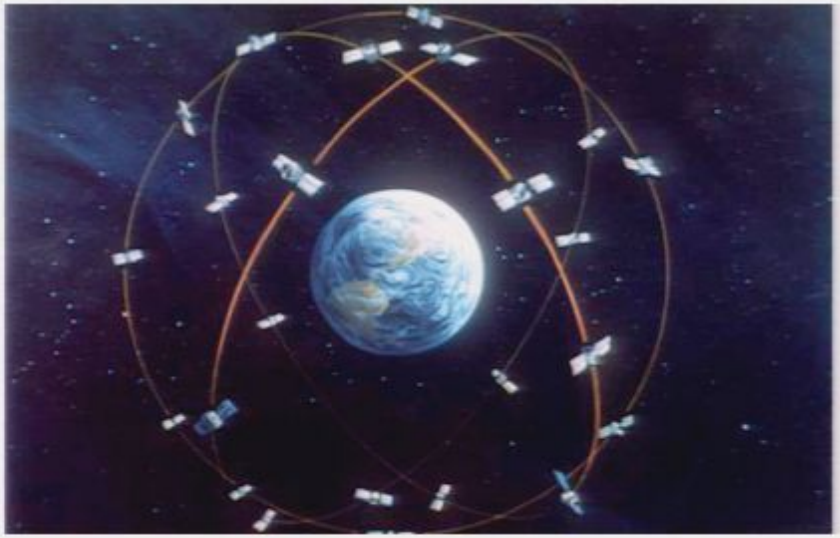

∫ f(t) × f


$\int f(t) \times f_{\text{impulse}} = ?$

$$\int f(t) \times f_{\text{impulse}} = \begin{matrix} + \\ 0 \end{matrix}$$

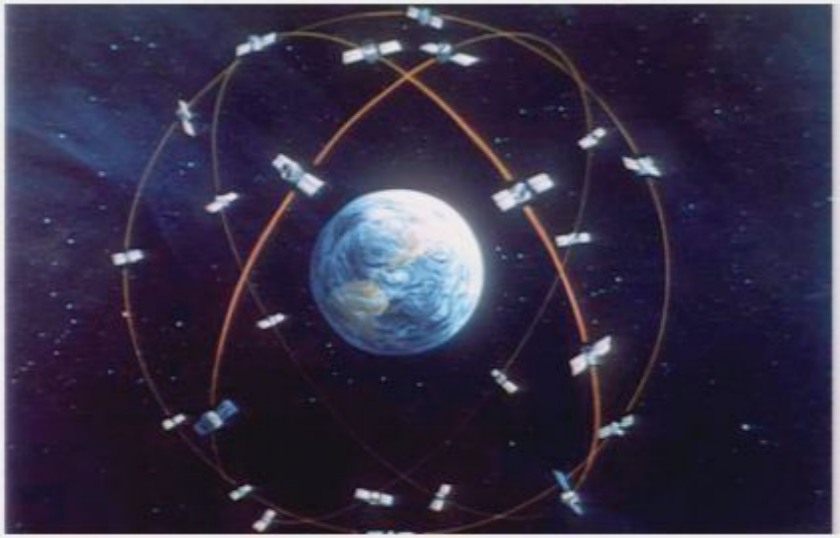


Communication Theory



- Lets us lock on to GPS satellites.
- How to communicate despite noise
  - *transmitting information through noisy channels*

Communication Theory



- Lets us lock on to GPS satellites.

- How to communicate despite noise
  - *transmitting information through noisy channels*

- E.g., can calculate a channel's *capacity*
  => *fundamental limit on transmission rate.*

Computation
(a.k.a *transforming* information)

Computation
(a.k.a *transforming* information)

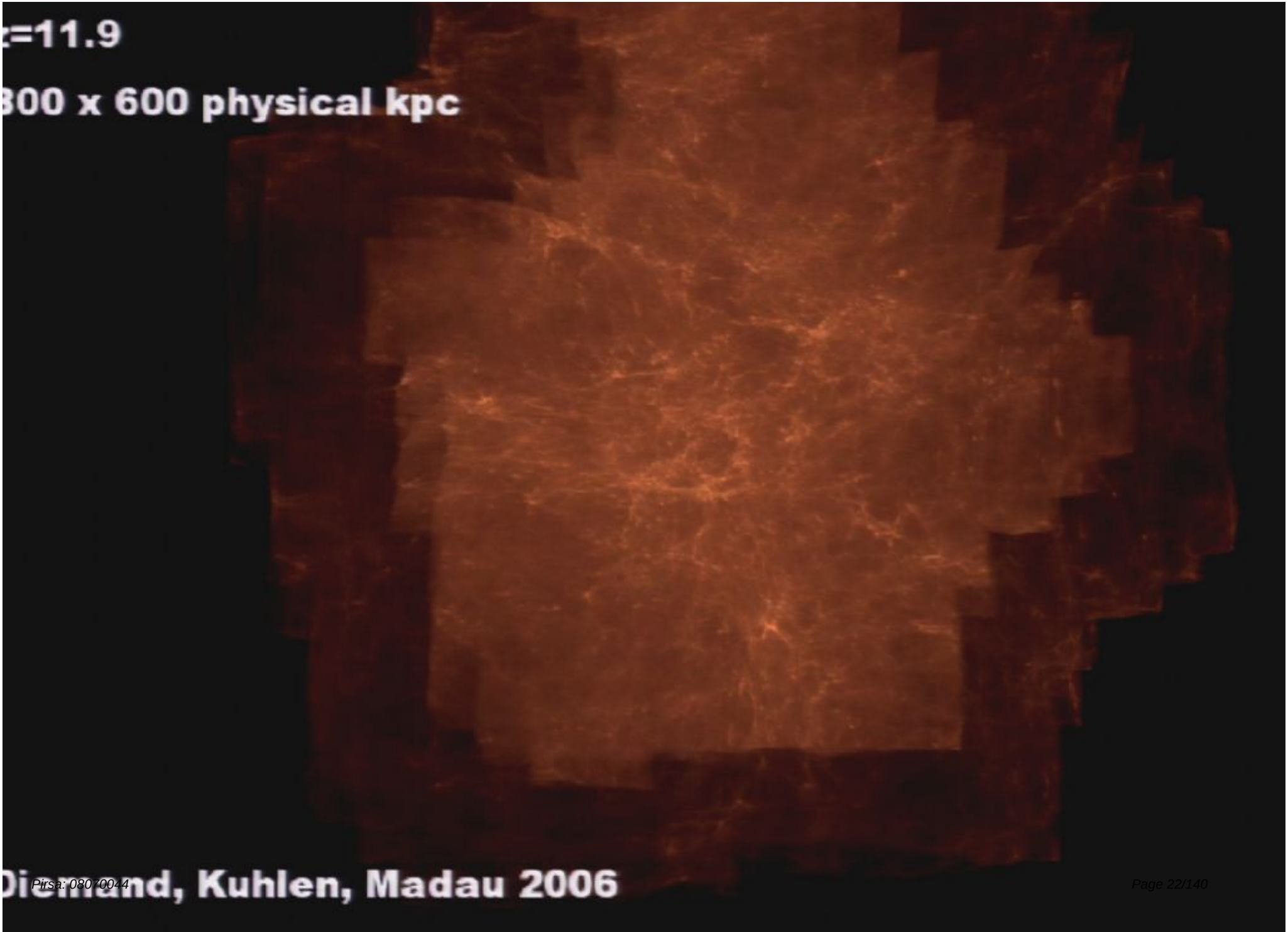
- Multiplication: {x,y} ⇒ xy

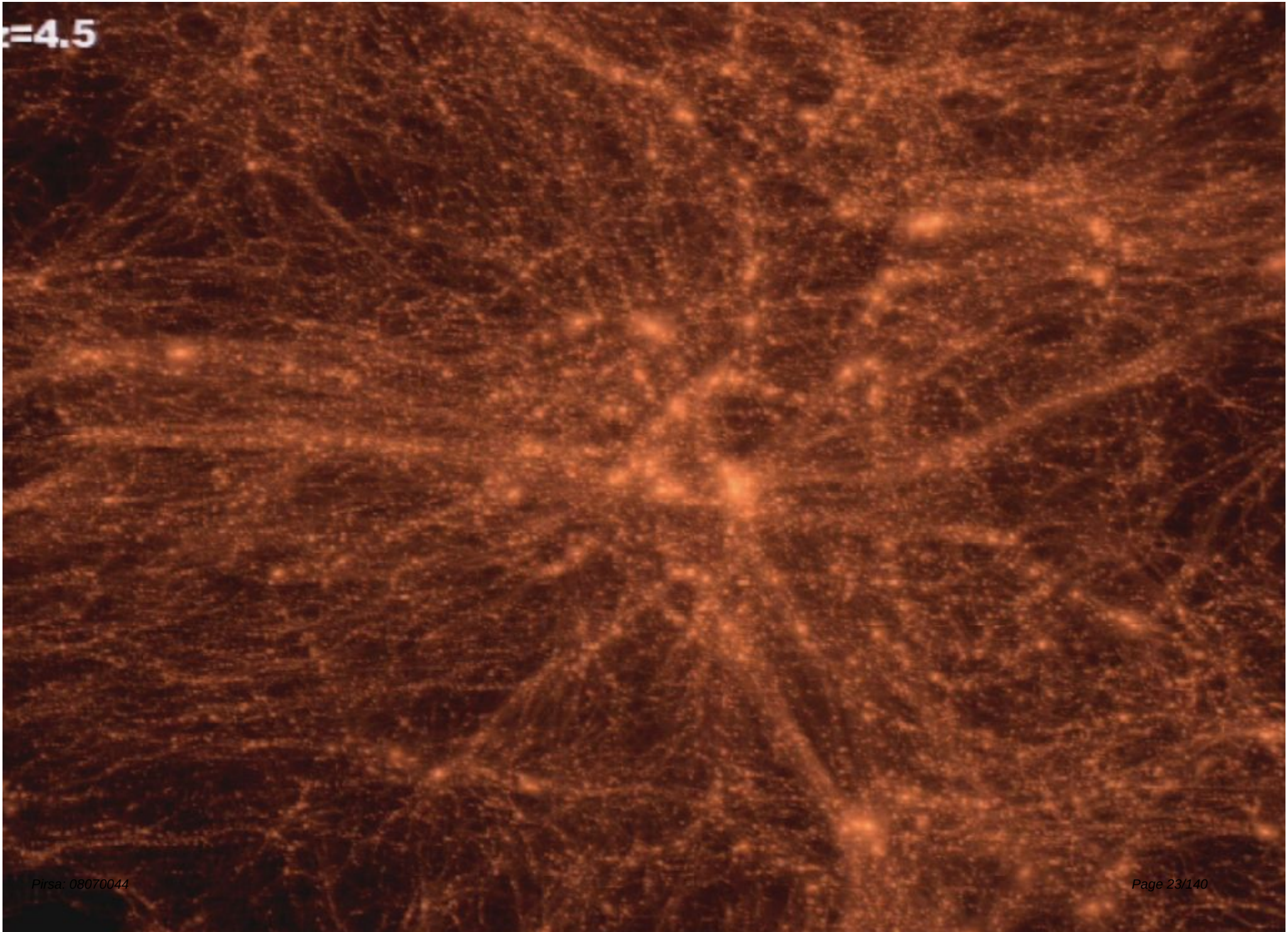
Computation
(a.k.a *transforming* information)

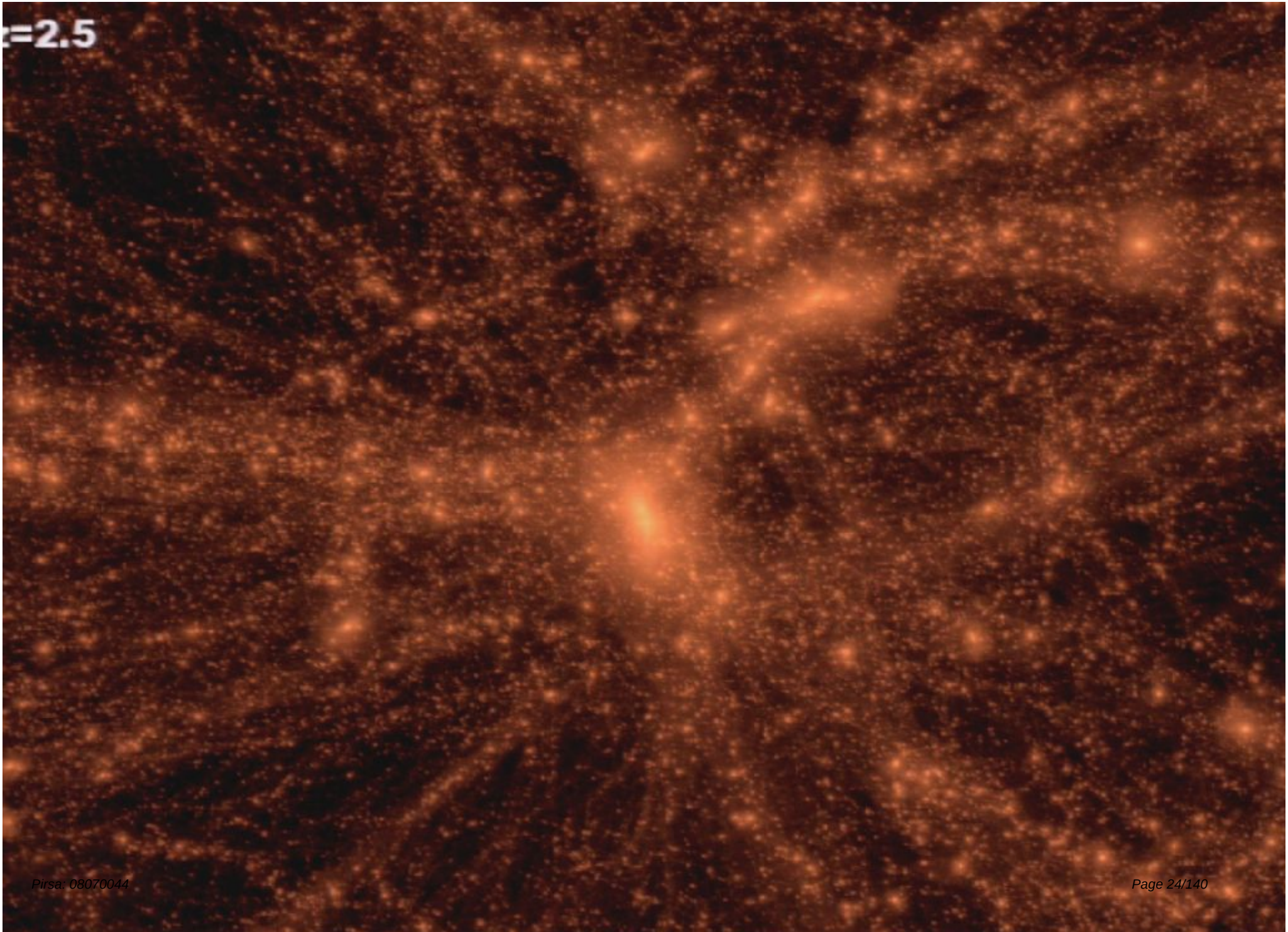
- Multiplication: {x,y} ⇒ xy
- Rendering: {HTML} ⇒ {web page}

Computation
(a.k.a *transforming* information)

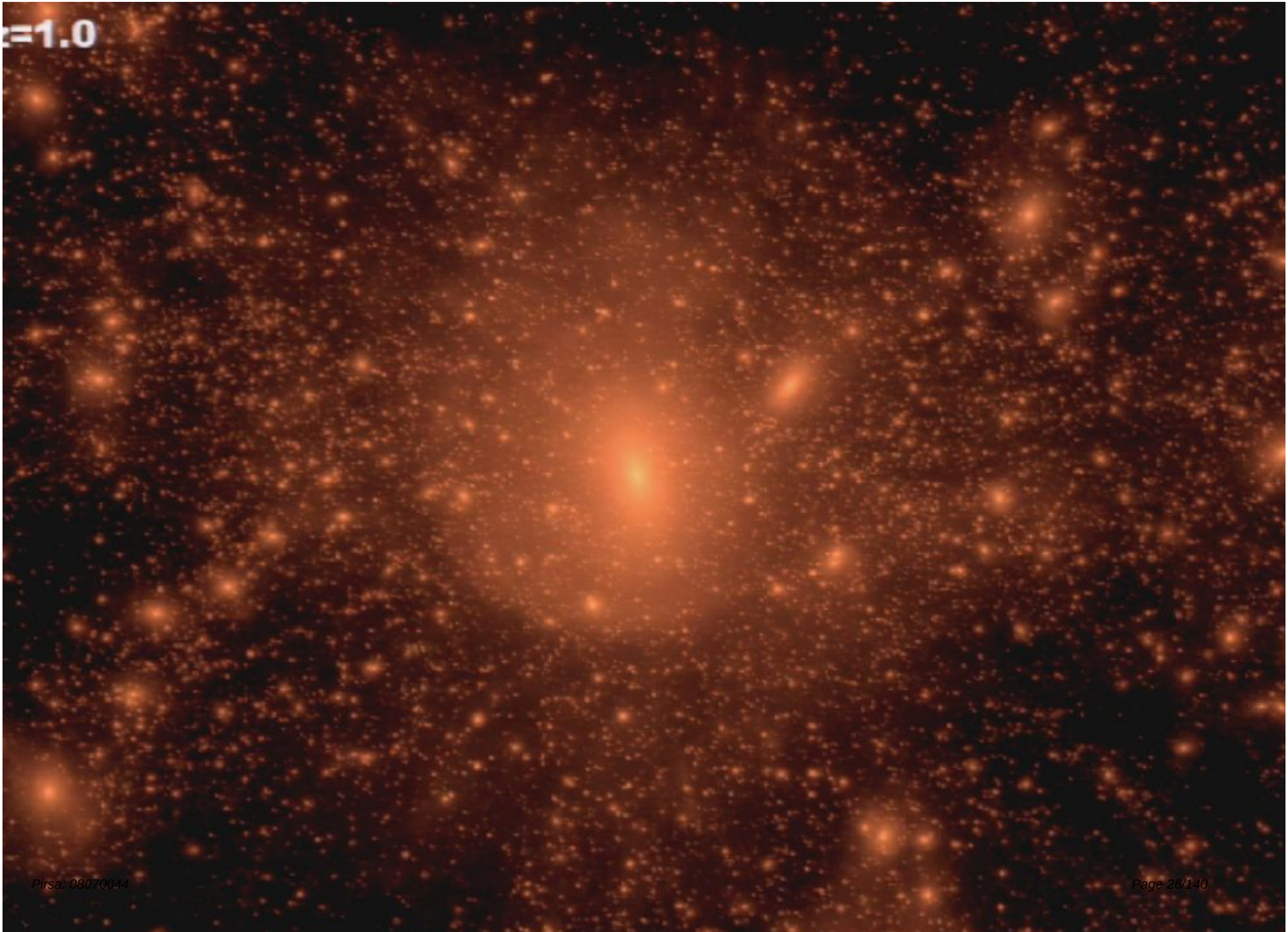
- Multiplication: {x,y} ⇒ xy
- Rendering: {HTML} ⇒ {web page}
- Simulation: {random gas atoms + gravity} ⇒ {galaxy formation}


z=11.9
300 x 600 physical kpc
Diemand, Kuhlen, Madau 2006


z=4.5


z=2.5


z=1.7

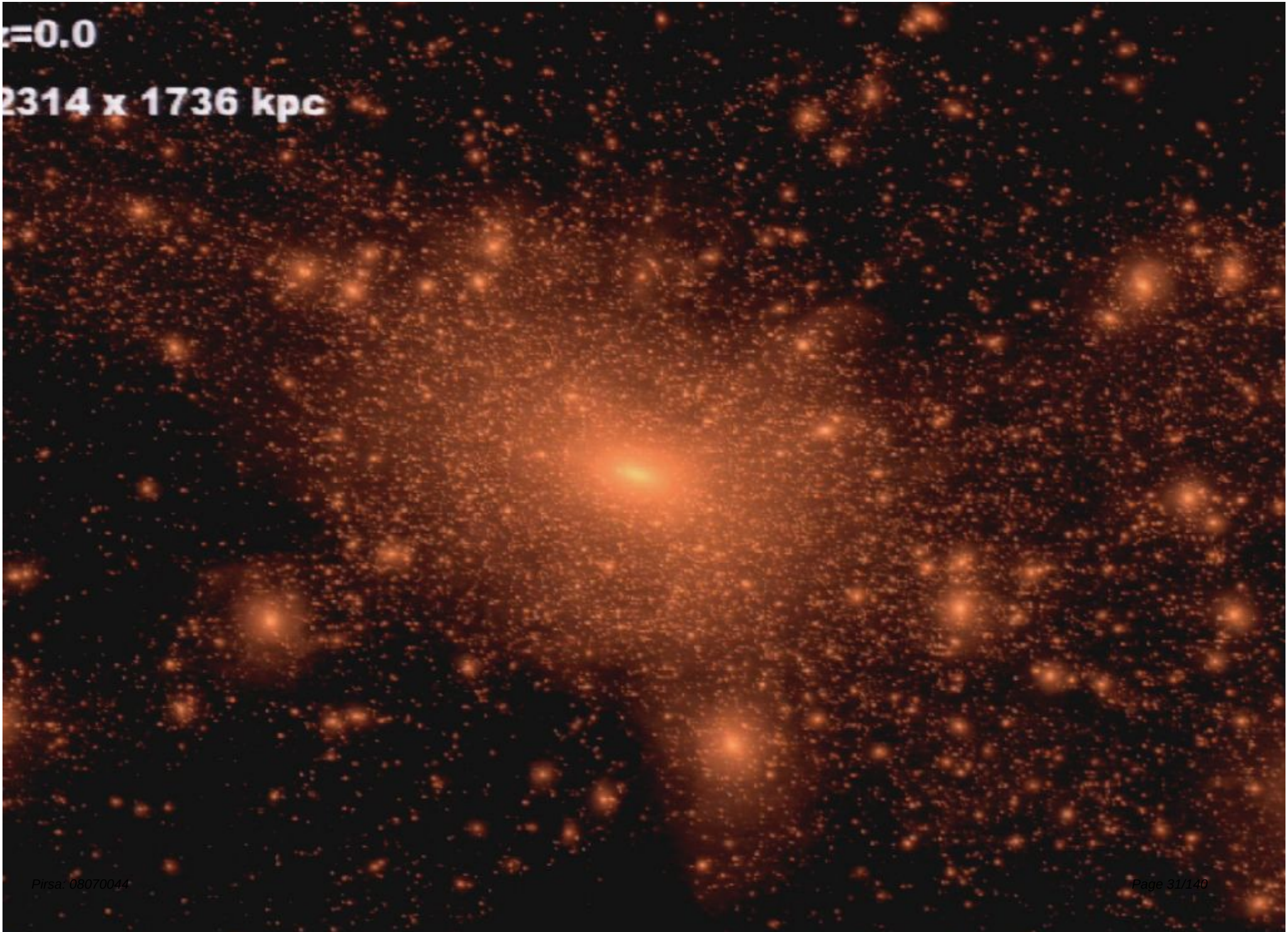

z=1.0


z=0.6


z=0.4


z=0.2

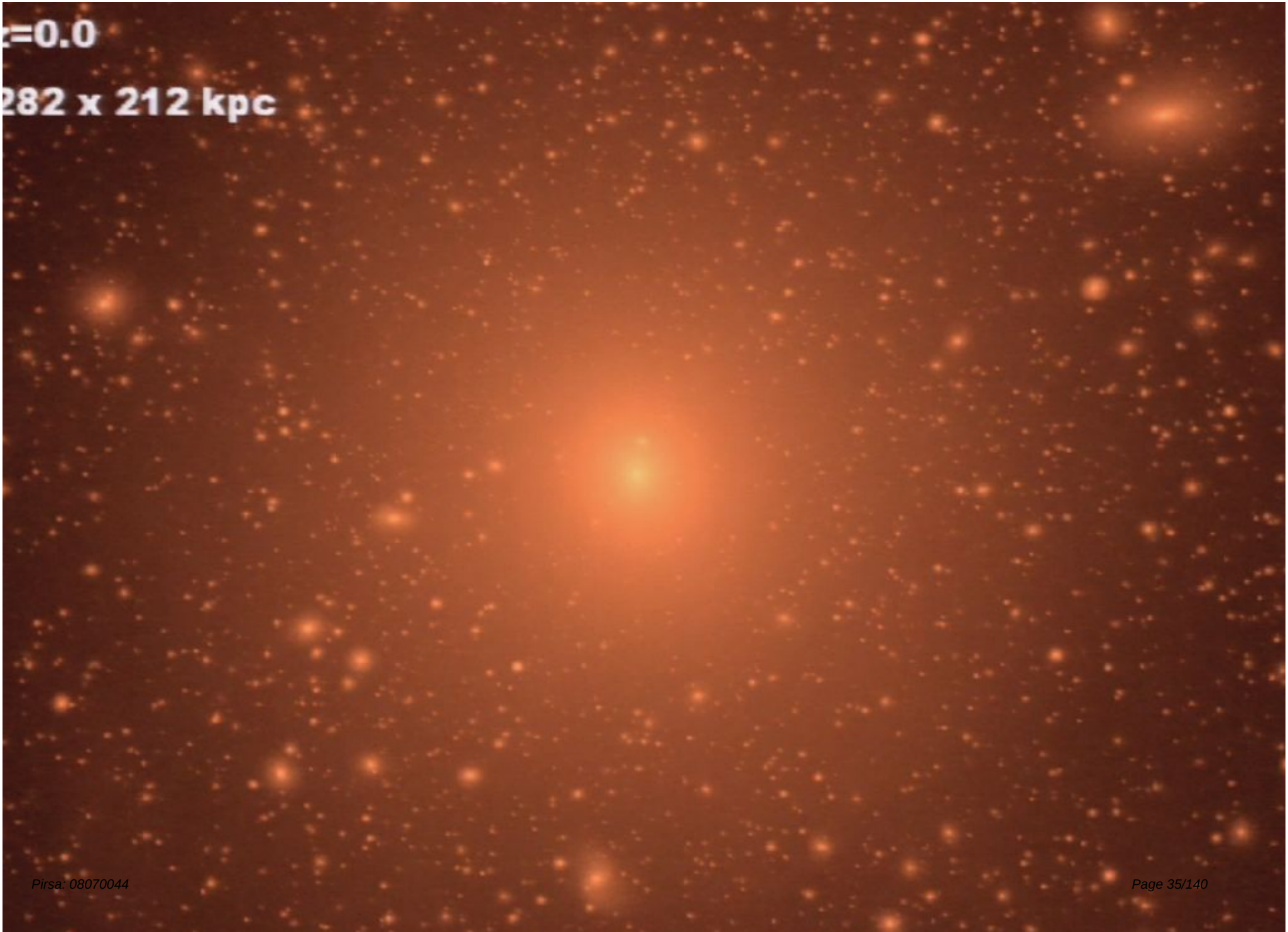

z=0.0


z=0.0
2314 x 1736 kpc


z=0.0
3659 x 2745 kpc


z=0.0
1770 x 1327 kpc


z=0.0
620 x 465 kpc


z=0.0
282 x 212 kpc


z=0.0
142 x 107 kpc
FNSNF
Fonds national suisse
Schweizerischer Nationalfonds
Fondo nazionale svizzero
Swiss National Science Foundation
NSF
UC SANTA CRUZ
NASA
Diemand, Kuhlen, Madau 2006

Computation
(a.k.a *transforming* information)

- Multiplication: {x,y} ⇒ xy
- Rendering: {HTML} ⇒ {web page}
- Simulation: {random gas atoms + gravity} ⇒ {galaxy formation}
- Factoring: xy ⇒ {x,y}

Computation
(a.k.a *transforming* information)

- Multiplication: {x,y} ⇒ xy
- Rendering: {HTML} ⇒ {web page}
- Simulation: {random gas atoms + gravity} ⇒ {galaxy formation}
- Factoring: xy ⇒ {x,y}
- Some problems are harder than others...

Computation
(a.k.a *transforming* information)

- Multiplication: {x,y} ⇒ xy $O(n \log n)$
- Rendering: {HTML} ⇒ {web page}
- Simulation: {random gas atoms + gravity} ⇒ {galaxy formation}
- Factoring: xy ⇒ {x,y}
- Some problems are harder than others...

Computation
(a.k.a *transforming* information)

- Multiplication: {x,y} ⇒ xy $O(n \log n)$
- Rendering: {HTML} ⇒ {web page} $O(n)$
- Simulation: {random gas atoms + gravity} ⇒ {galaxy formation} $O(n^2)$
- Factoring: xy ⇒ {x,y}
- Some problems are harder than others...

Cryptography
(a.k.a. communicating *secretly*)

Cryptography
(a.k.a. communicating *secretly*)

- Caesar cypher: "hello world" ⇒ "ifmmp xpsme"

Scorecard: easy, convenient, totally insecure

Cryptography
(a.k.a. communicating *secretly*)

- Caesar cypher: "hello world" ⇒ "ifmmp xpsme"

  Scorecard: easy, convenient, totally insecure

- One-time pad: Sender XORs with a random *key*. Looks like gibberish until de-XORed.

  Scorecard: easy, awkward, absolutely secure

Cryptography
(a.k.a. communicating *secretly*)

- Caesar cypher: "hello world" ⇒ "ifmmp xpsme"

  Scorecard: easy, convenient, totally insecure

- One-time pad: Sender XORs with a random *key*. Looks like gibberish until de-XORed.

  Scorecard: easy, awkward, absolutely secure

- RSA *public-key* crypto: *Public* key (encryption) is x*y. *Private* key(decryption) is {x,y}

  Scorecard: complex, convenient, *computationally* secure

How Quantum is Different

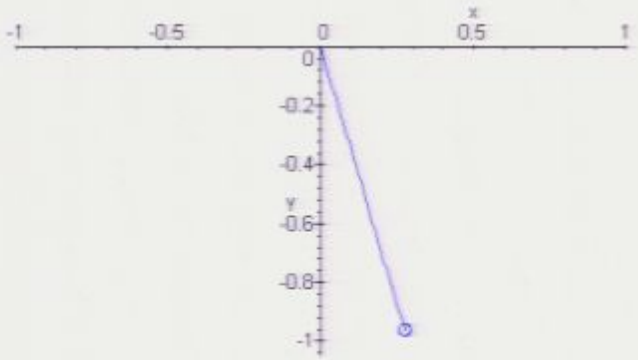
Nature is weirder than we thought (c. 1900)

- Experimental symptoms:
  * atoms don't collapse
  * light comes in chunks *and* it diffracts
  * glowing charcoal radiates *finite* energy
- Physical systems follow unexpected rules!
  * "*The particle has well-defined position and momentum*" is **not** true.
  * "*The photon's energy is an integer multiple of its frequency*" ***is*** *true.*
- Conclusion: We needed a new set of states to describe physical systems in our quantum world.

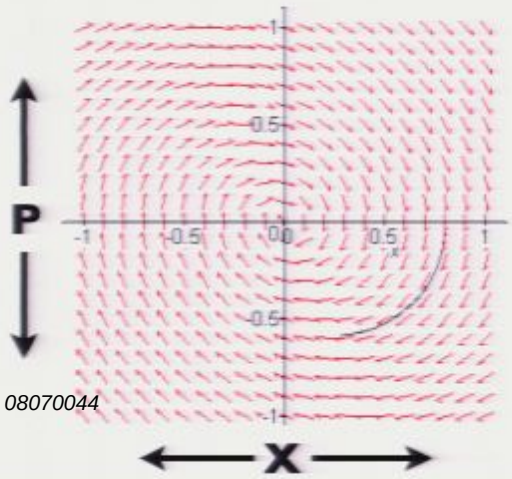
States of Classical Systems

Example I: Pendulum

Simple Pendulum in Real Space : Damped with Coeff = 0.4



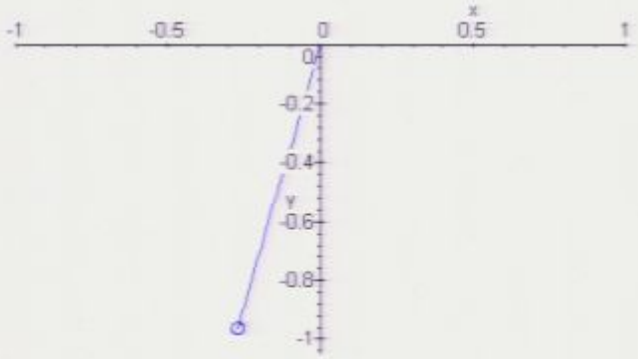
Simple Pendulum in Phase Space : Damped with Coef f= 0.4



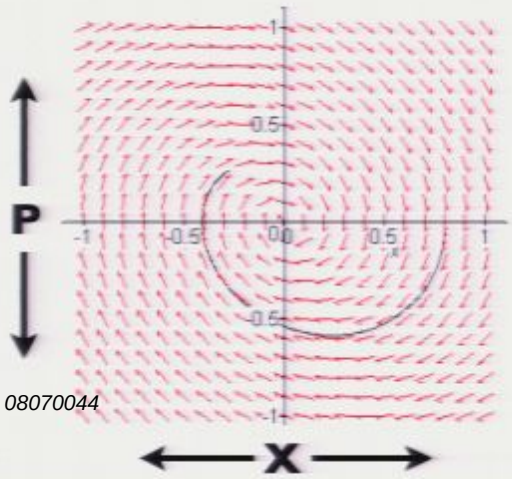
States of Classical Systems

Example 1: Pendulum

Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4

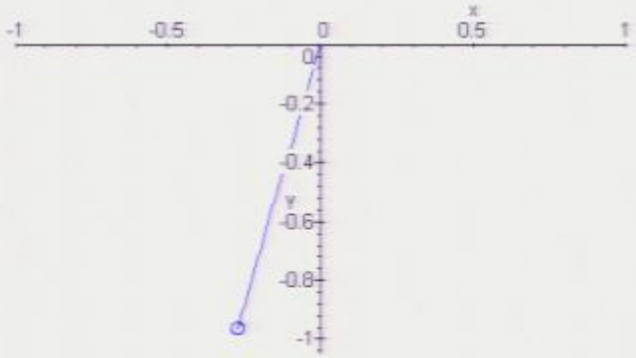


Example 2: A Switch

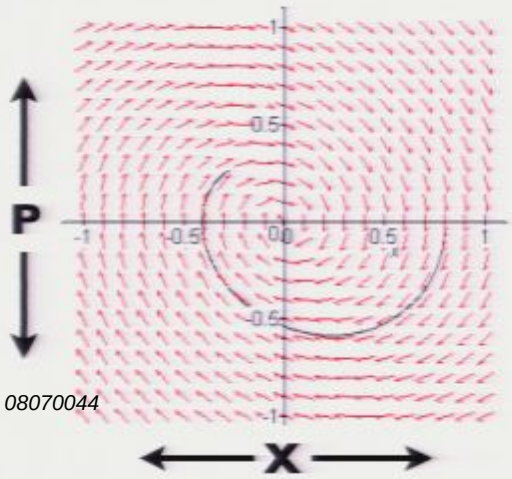
States of Classical Systems

Example 1: Pendulum

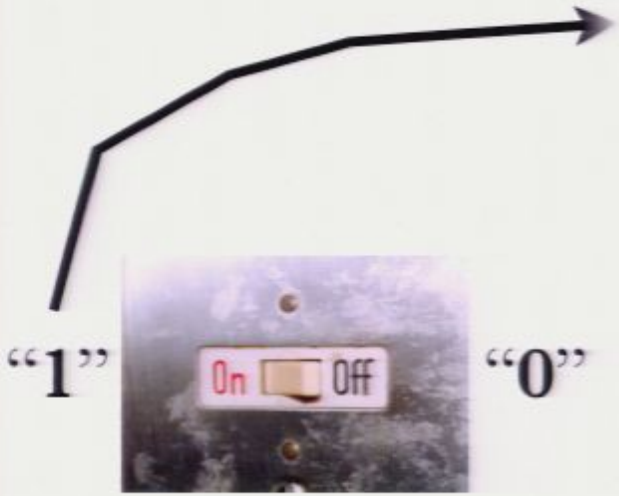
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4

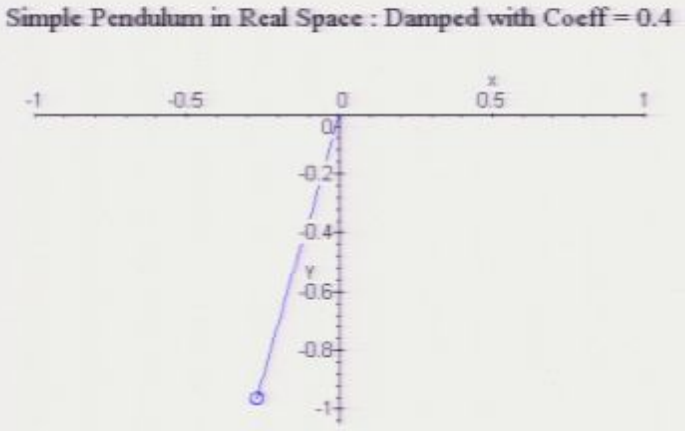


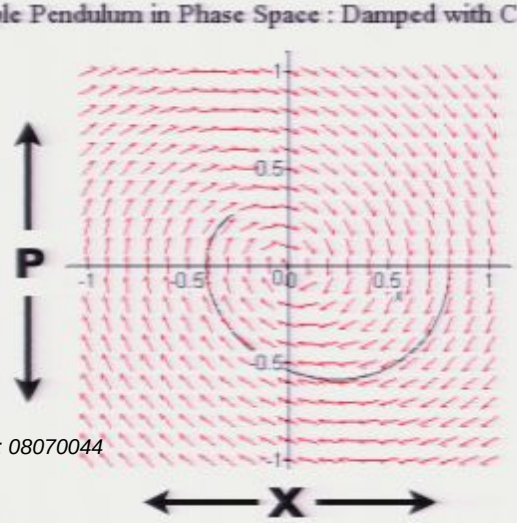
Example 2: A Switch



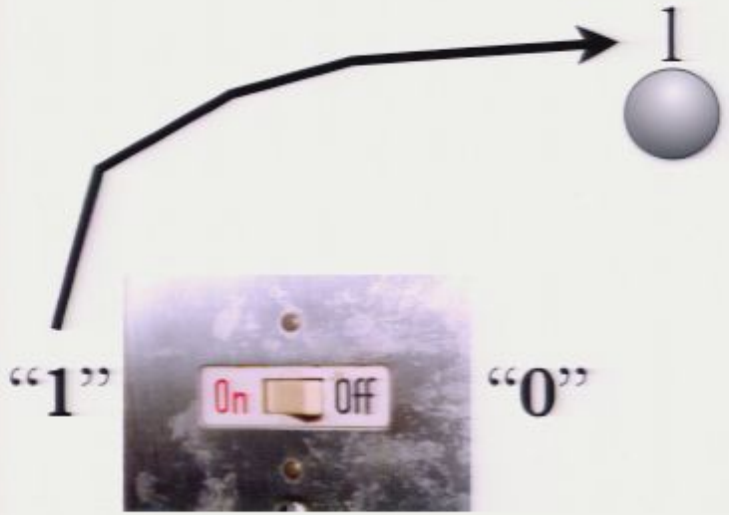
States of Classical Systems

Example 1: Pendulum





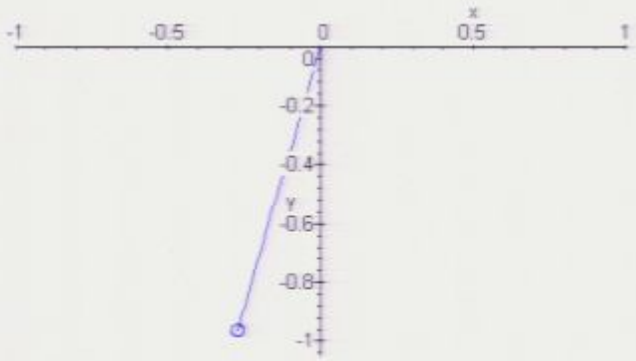
Example 2: A Switch



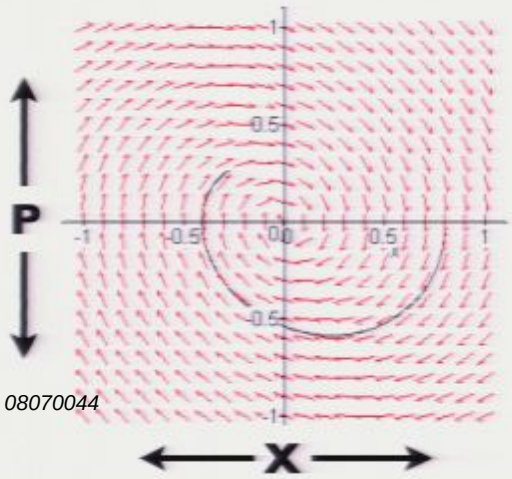
States of Classical Systems

Example 1: Pendulum

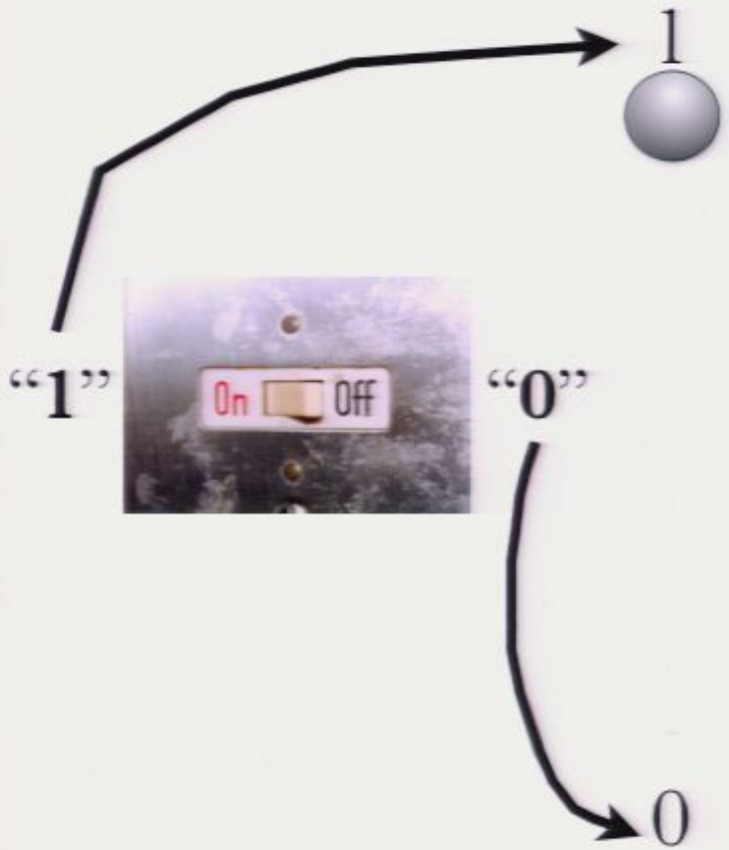
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4



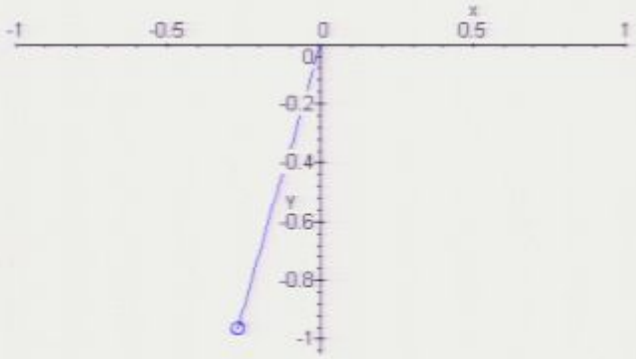
Example 2: A Switch



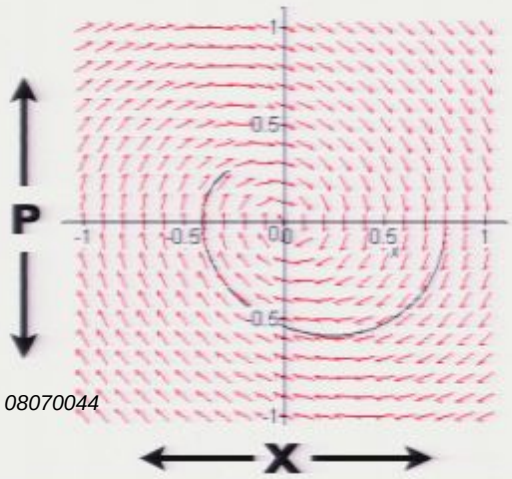
States of Classical Systems

Example 1: Pendulum

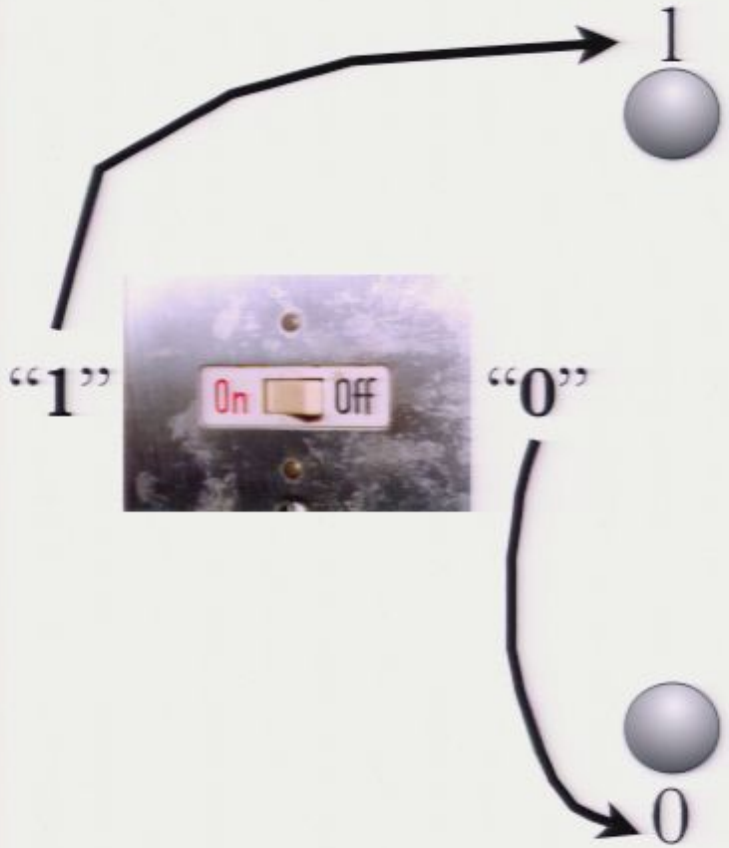
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4



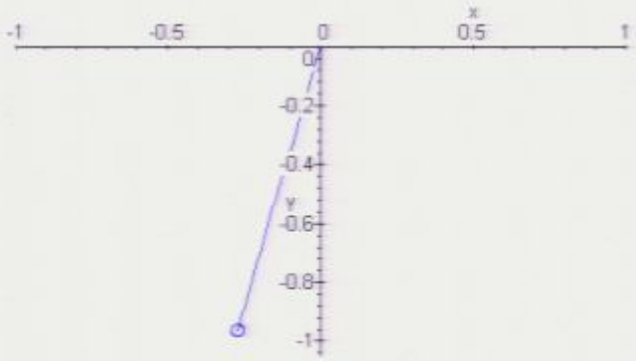
Example 2: A Switch



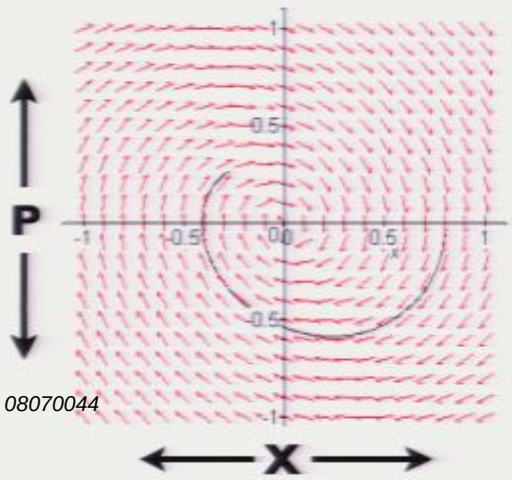
States of Classical Systems

Example 1: Pendulum

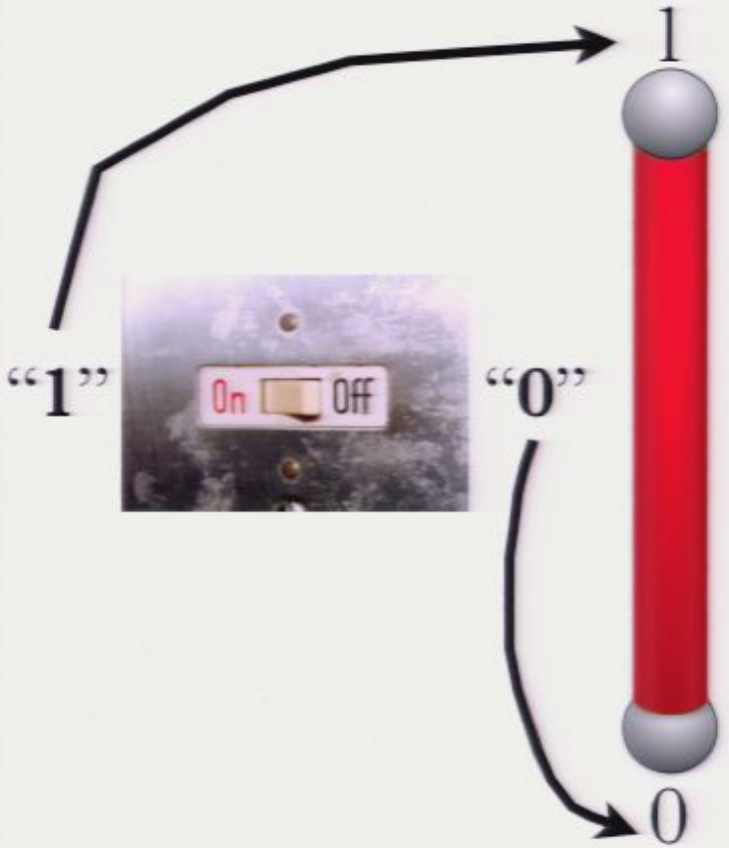
Simple Pendulum in Real Space : Damped with Coeff = 0.4

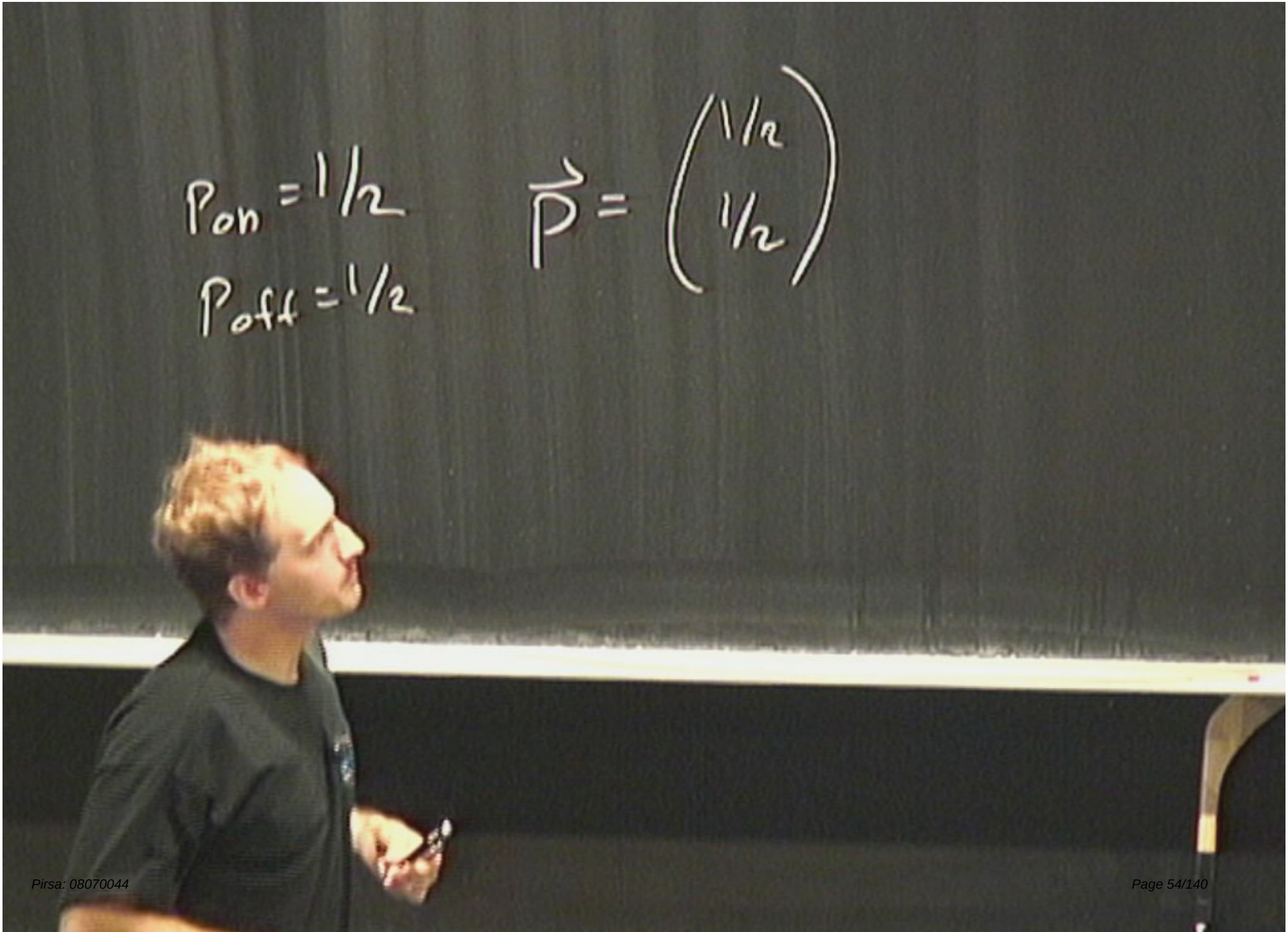


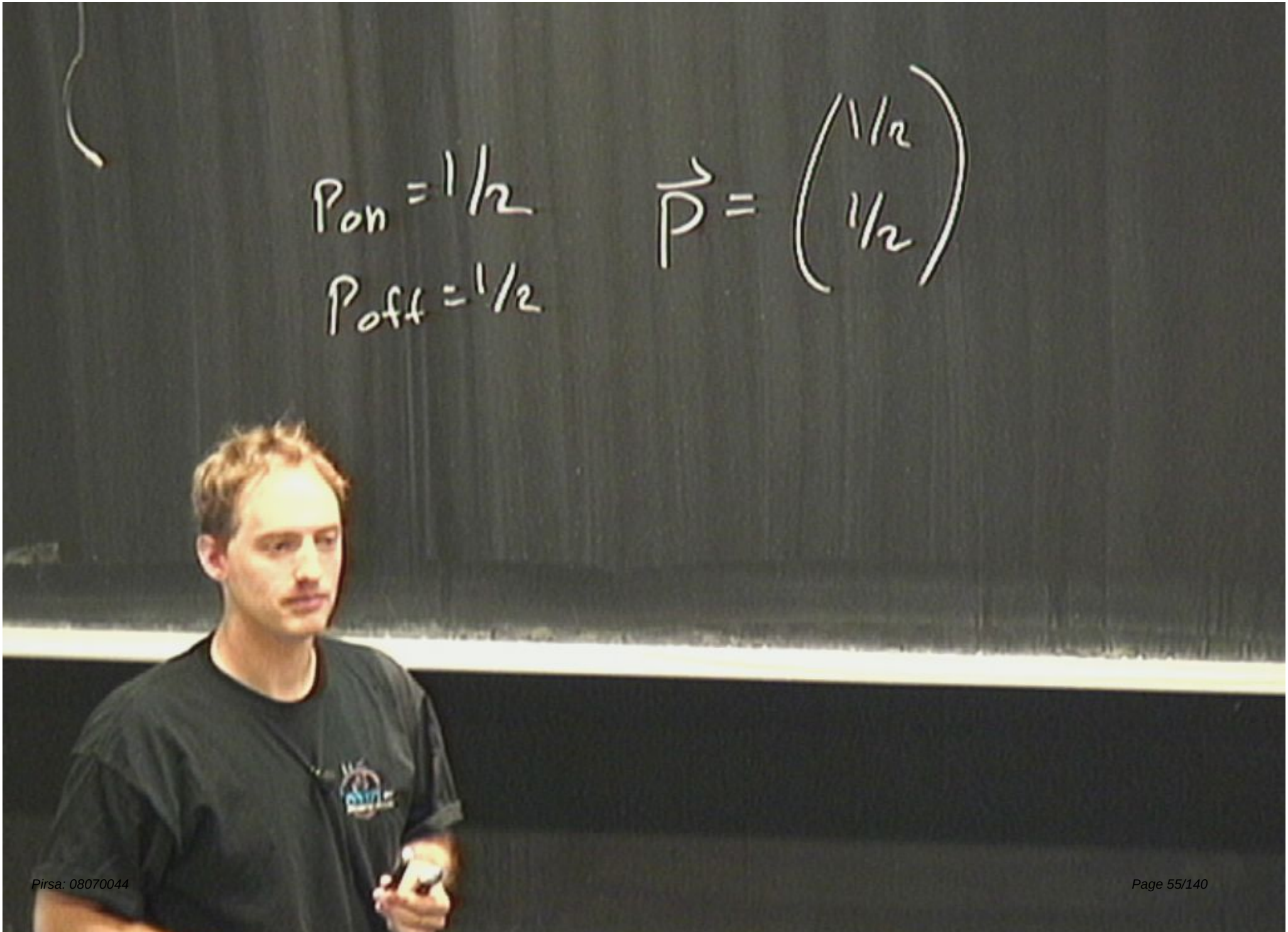
Simple Pendulum in Phase Space : Damped with Coef f= 0.4

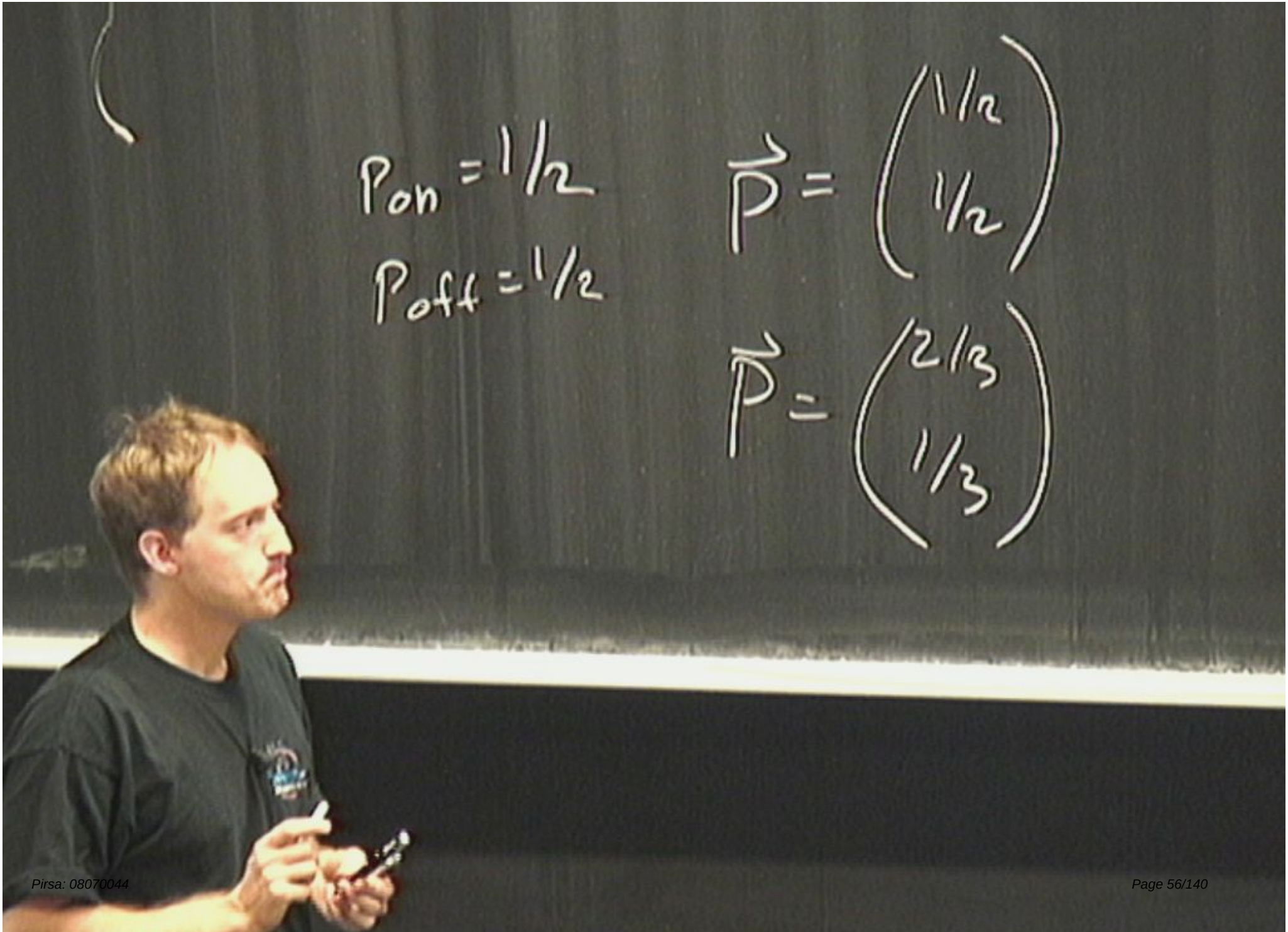


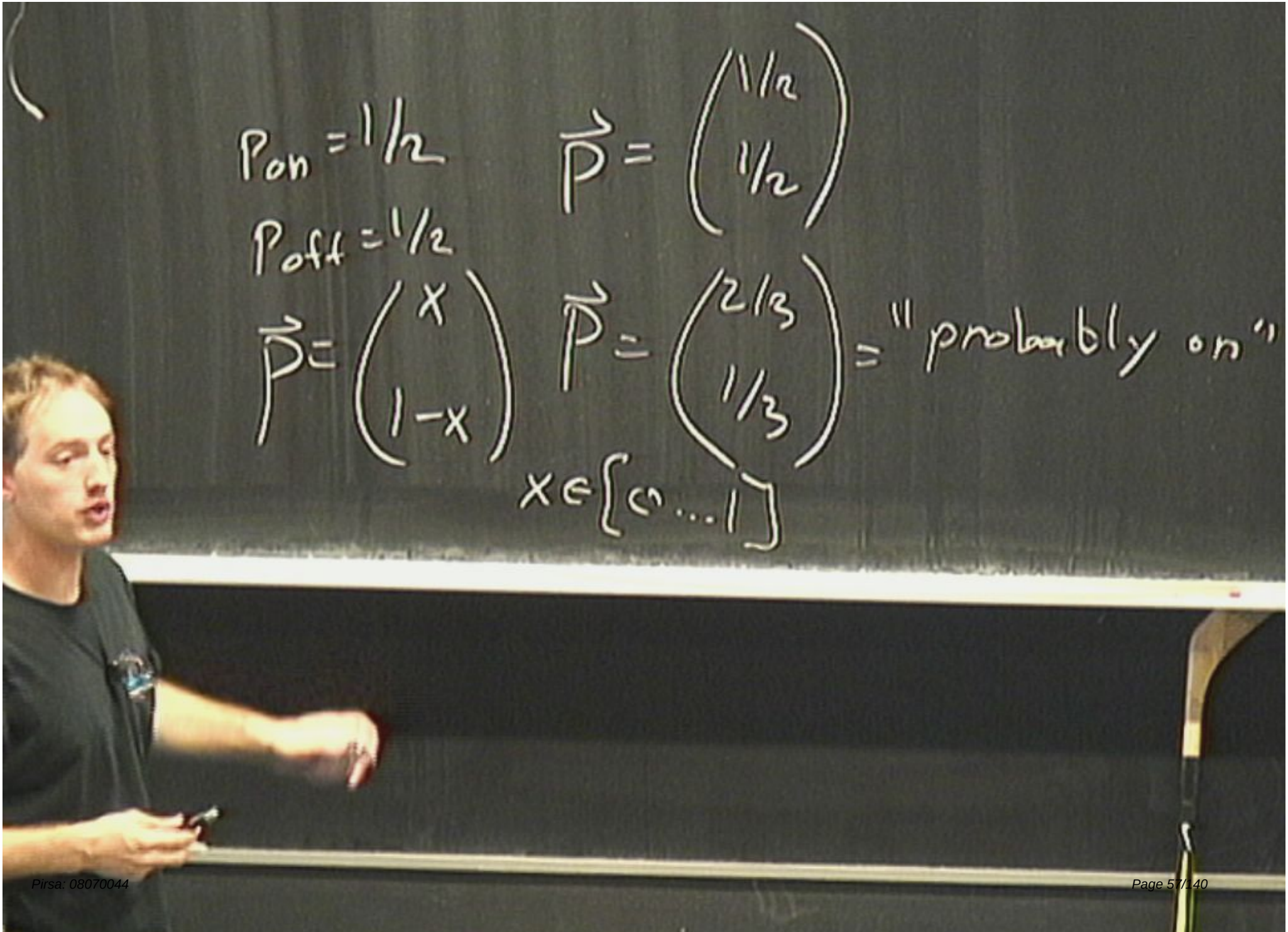
Example 2: A Switch




$P_{on} = 1/2$
$P_{off} = 1/2$
$\vec{p} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$

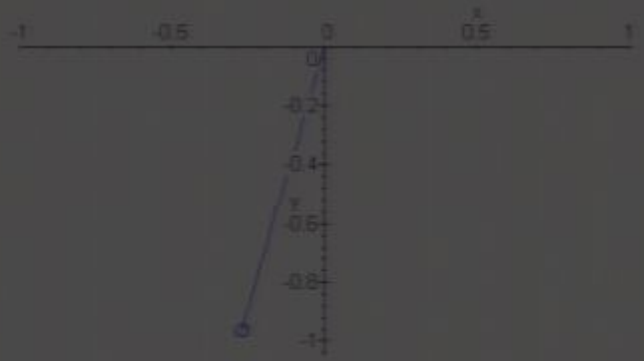

$P_{on} = 1/2$
$P_{off} = 1/2$
$\vec{p} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$

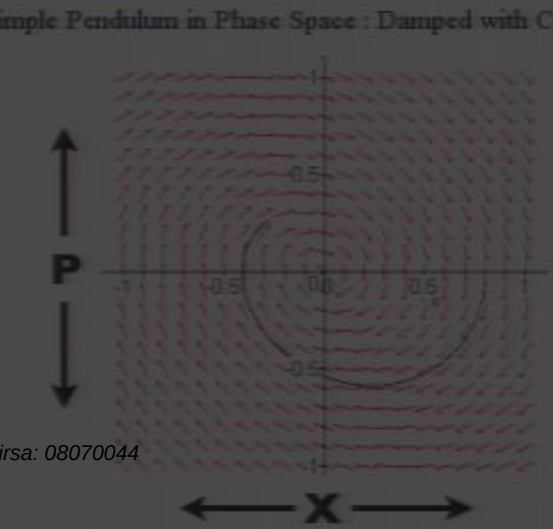

$P_{on} = 1/2$
$P_{off} = 1/2$
$\vec{P} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$
$\vec{P} = \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}$


$P_{on} = 1/2$
$P_{off} = 1/2$
$\vec{p} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$
$\vec{p} = \begin{pmatrix} x \\ 1-x \end{pmatrix}$
$\vec{p} = \begin{pmatrix} 2/3 \\ 1/3 \end{pmatrix}$ = "probably on"
$x \in [0 \ldots 1]$

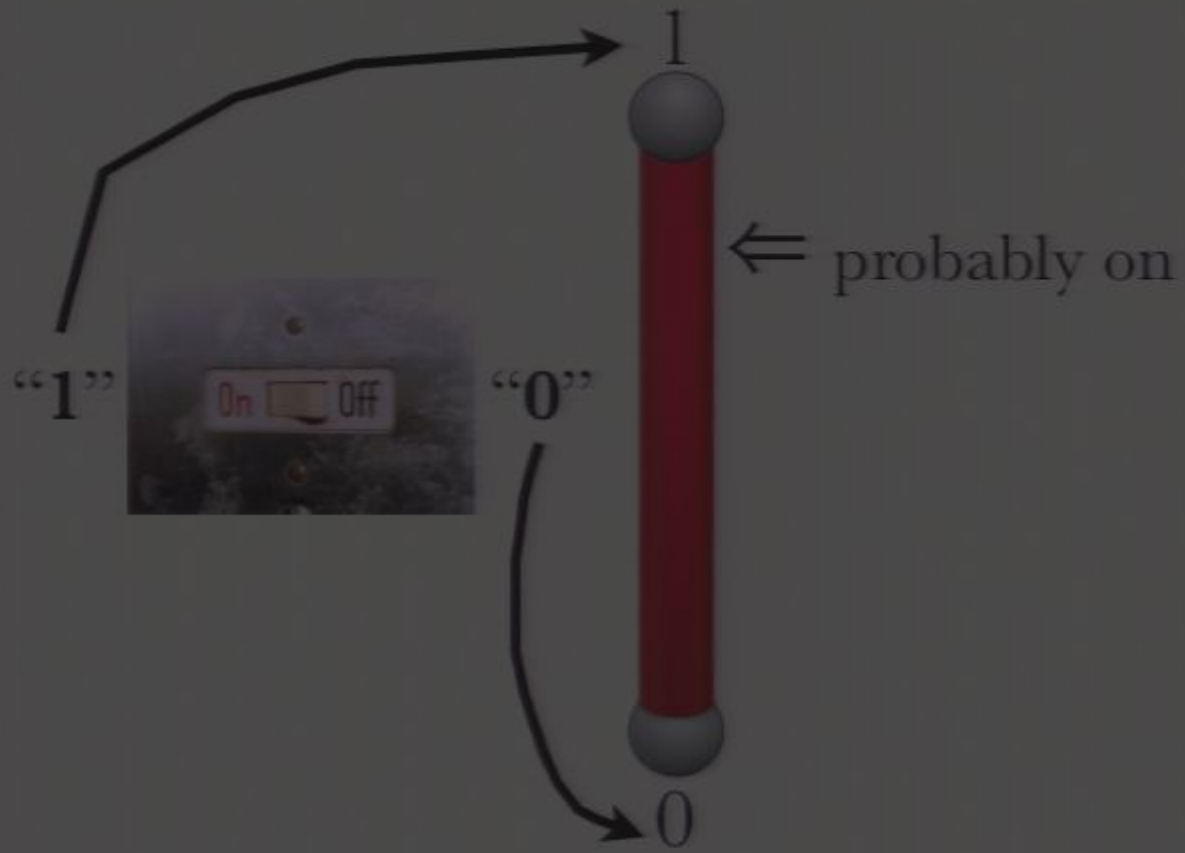
States of Classical Systems

Example 1: Pendulum





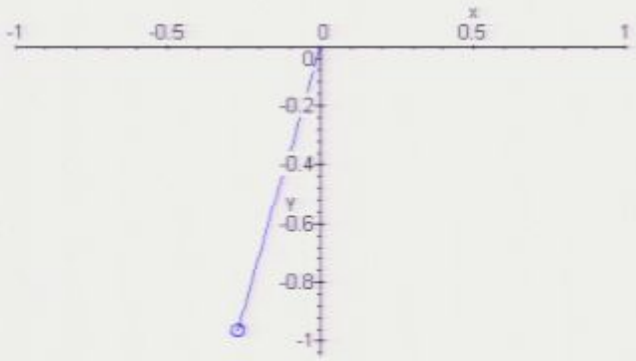
Example 2: A Switch



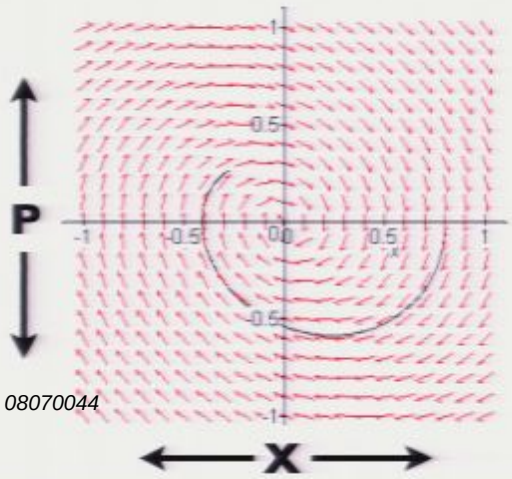
States of Classical Systems

Example 1: Pendulum

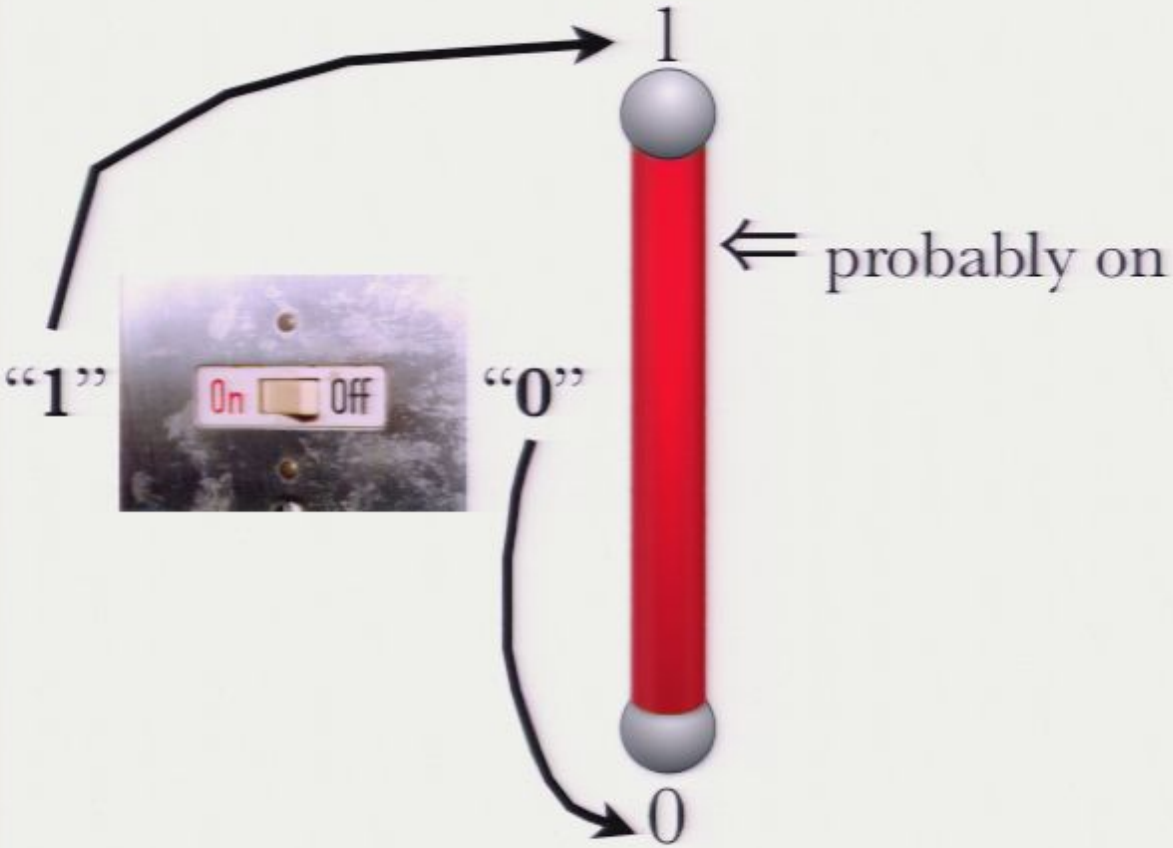
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4



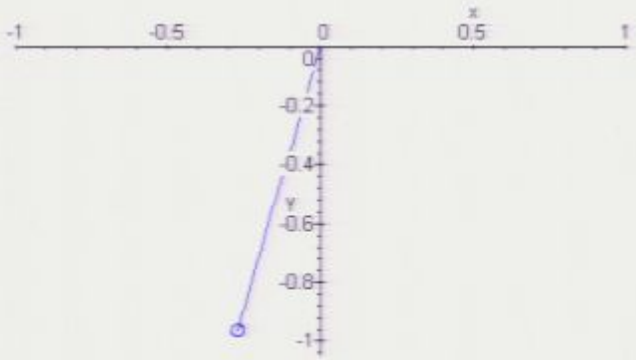
Example 2: A Switch



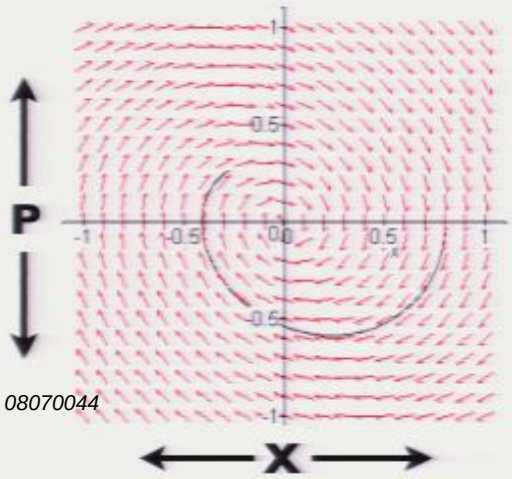
States of Classical Systems

Example 1: Pendulum

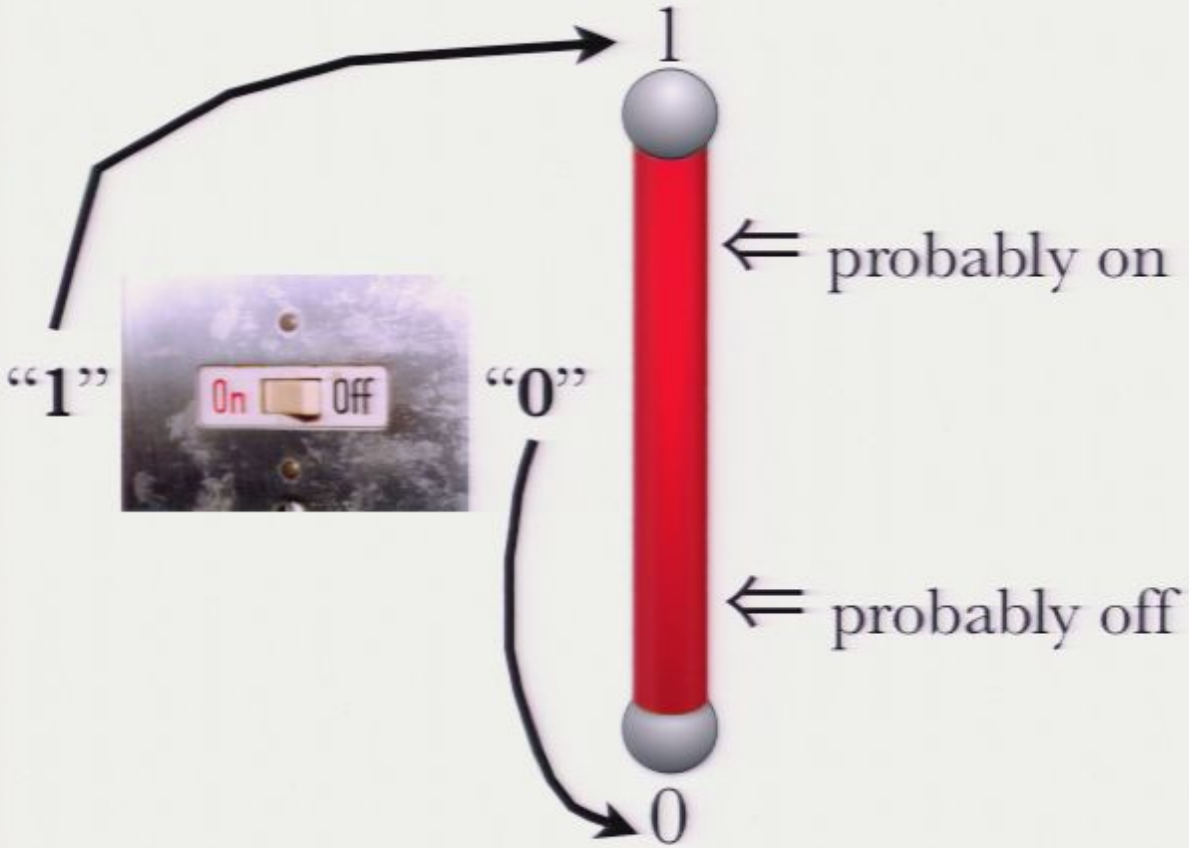
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4



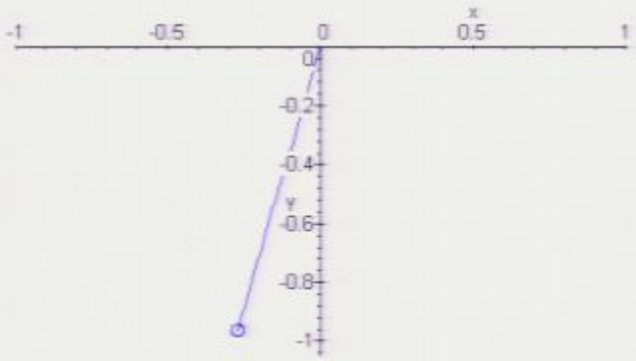
Example 2: A Switch



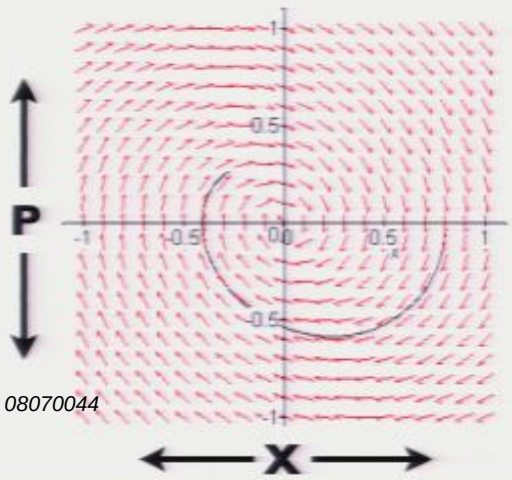
States of Classical Systems

Example 1: Pendulum

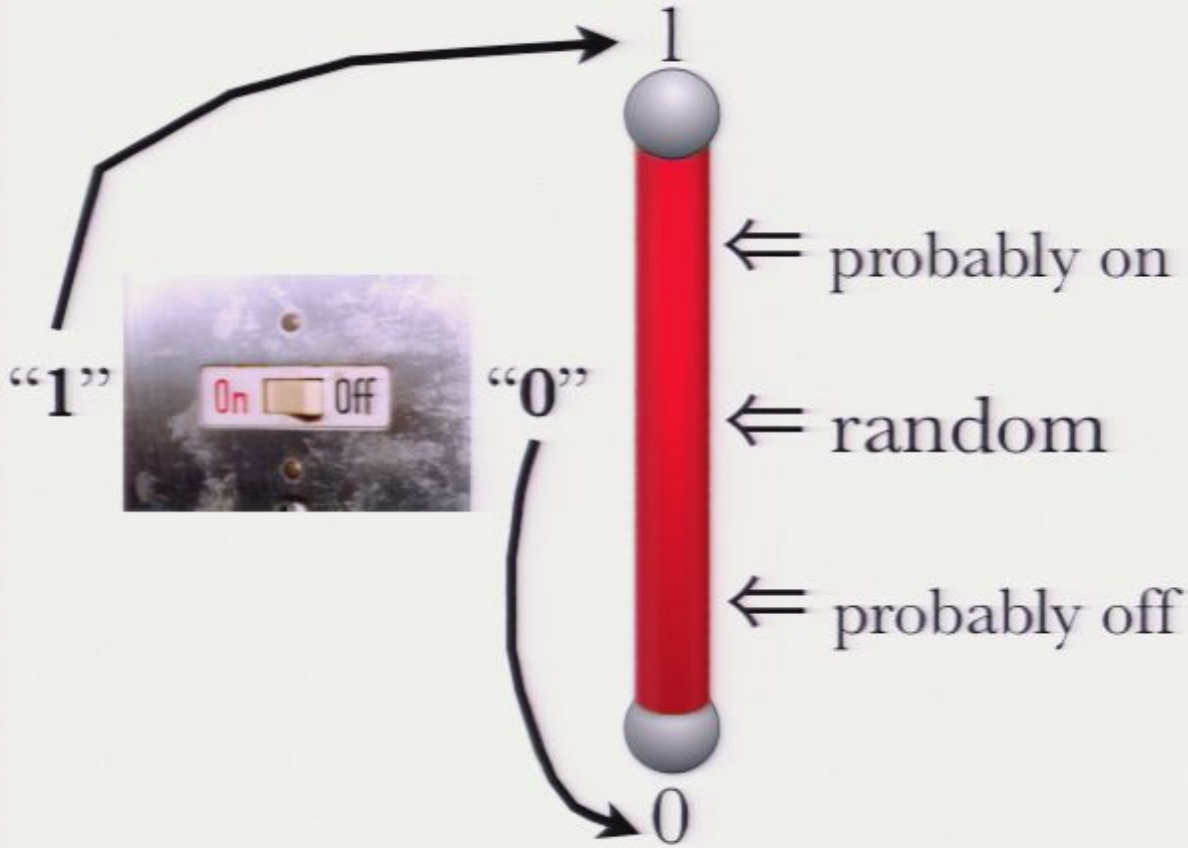
Simple Pendulum in Real Space : Damped with Coeff = 0.4



Simple Pendulum in Phase Space : Damped with Coef f= 0.4

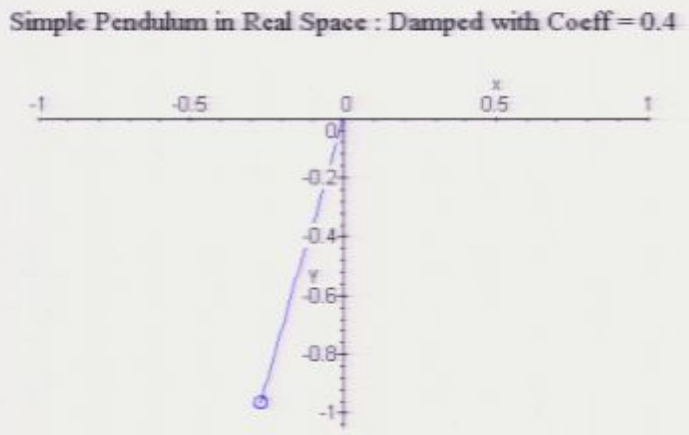


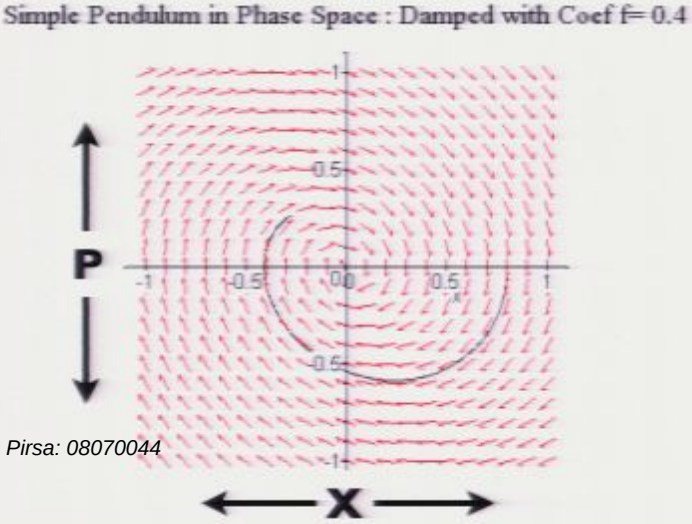
Example 2: A Switch



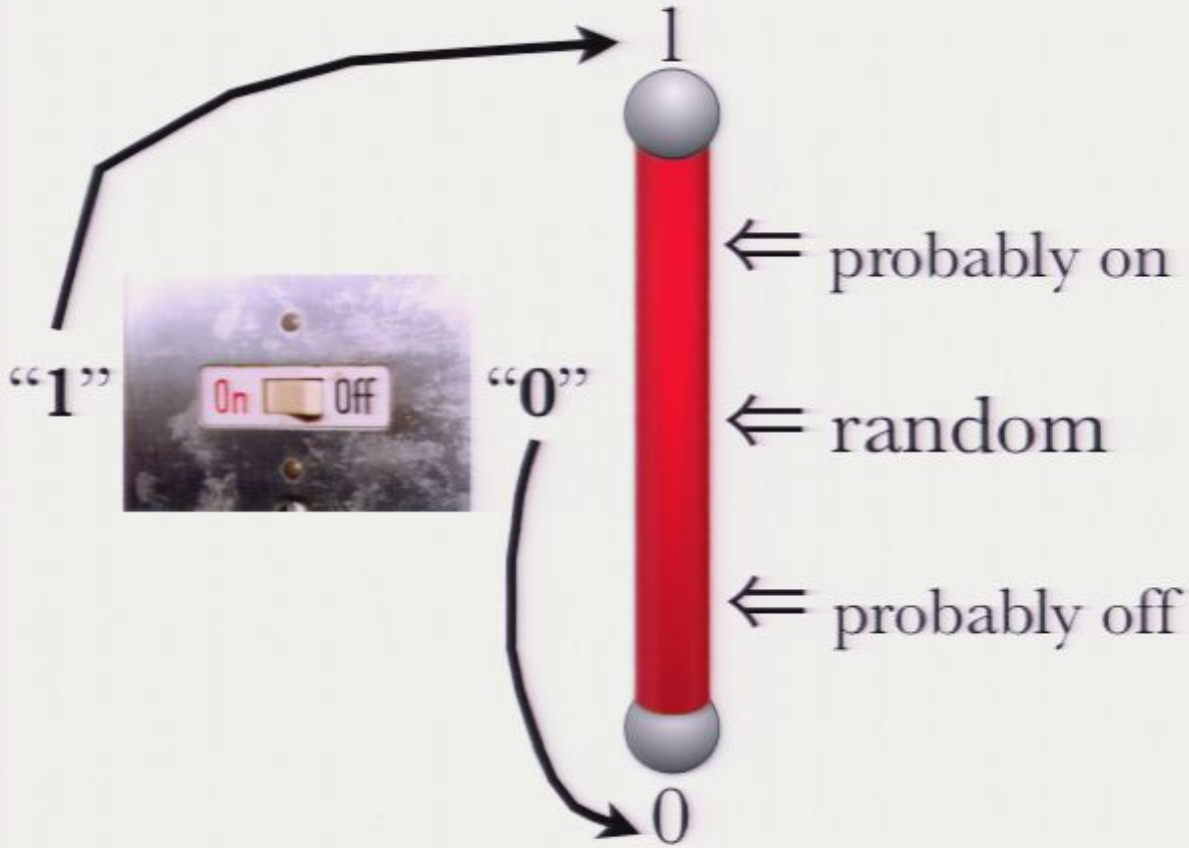
States of Classical Systems

Example 1: Pendulum





Example 2: A Switch



***Reversible* dynamics = permutations of {0,1}.**

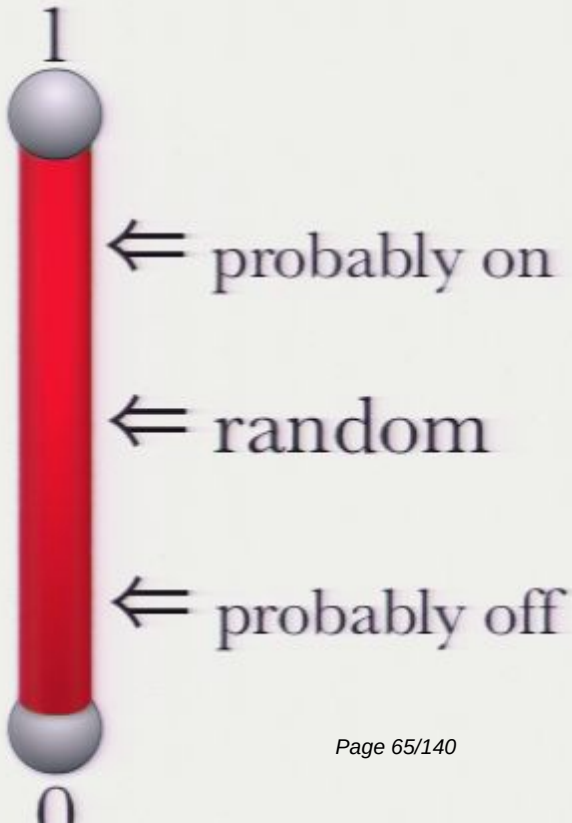
Hardy's Axiom

Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."

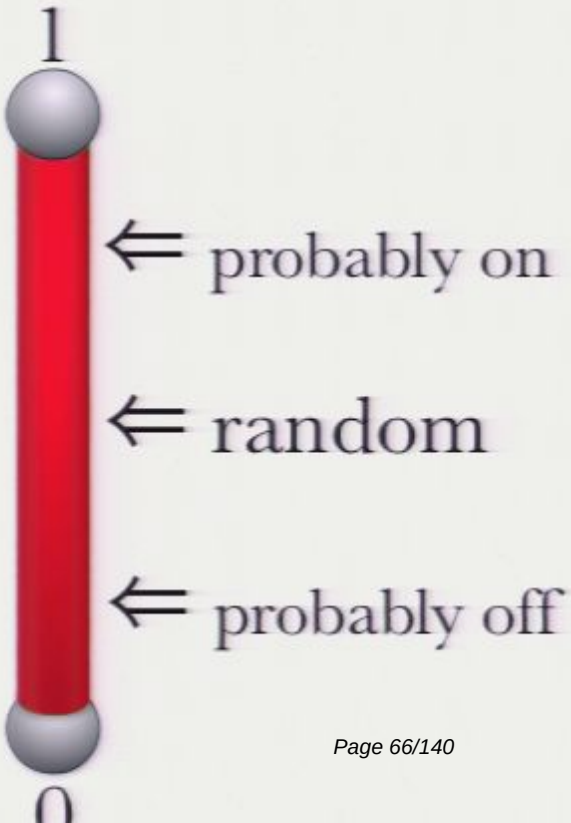
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."



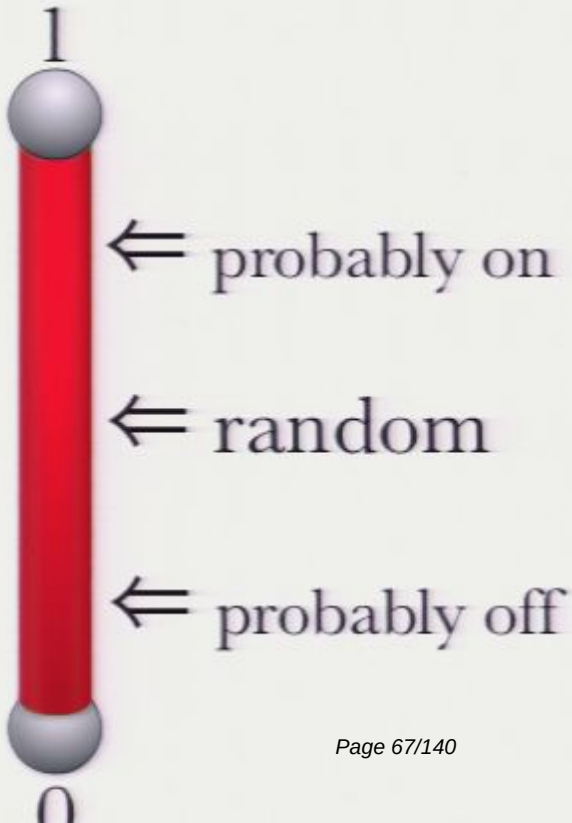
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!



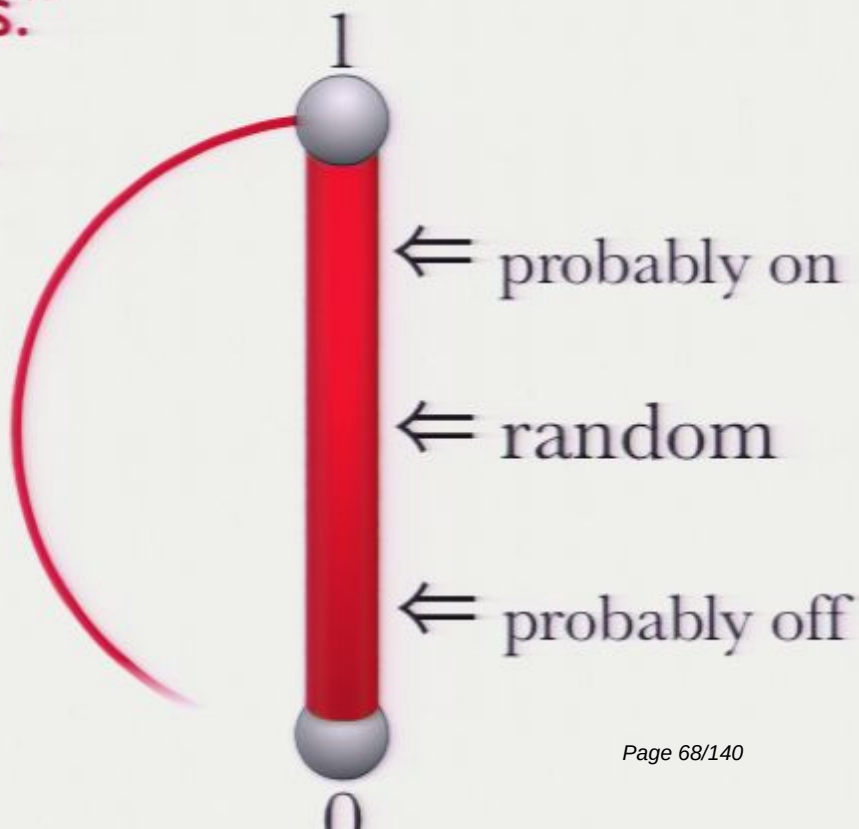
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...



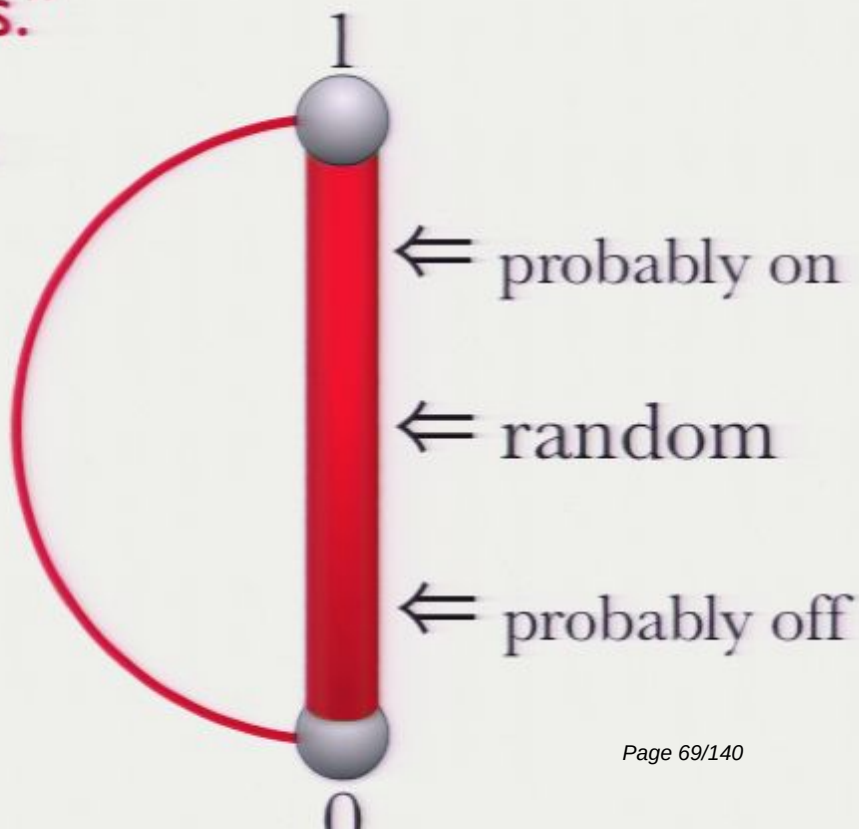
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...



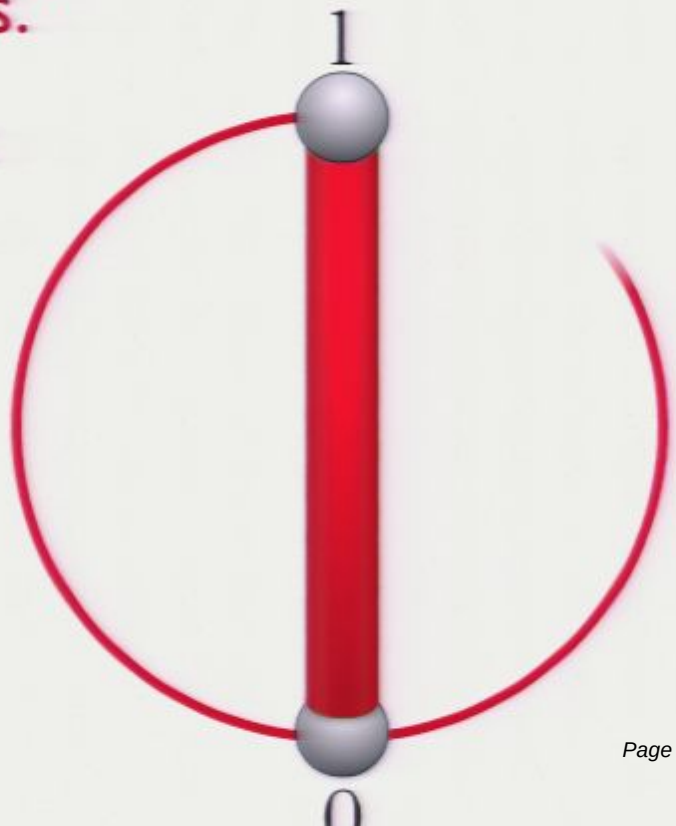
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...
- ...and even more to go from 0 back to 1...



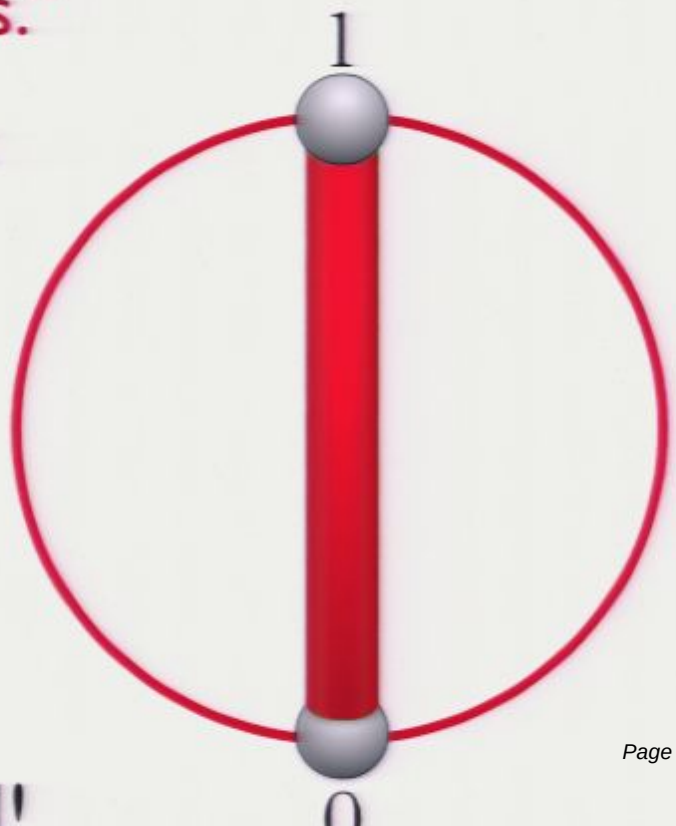
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...
- ...and even more to go from 0 back to 1...



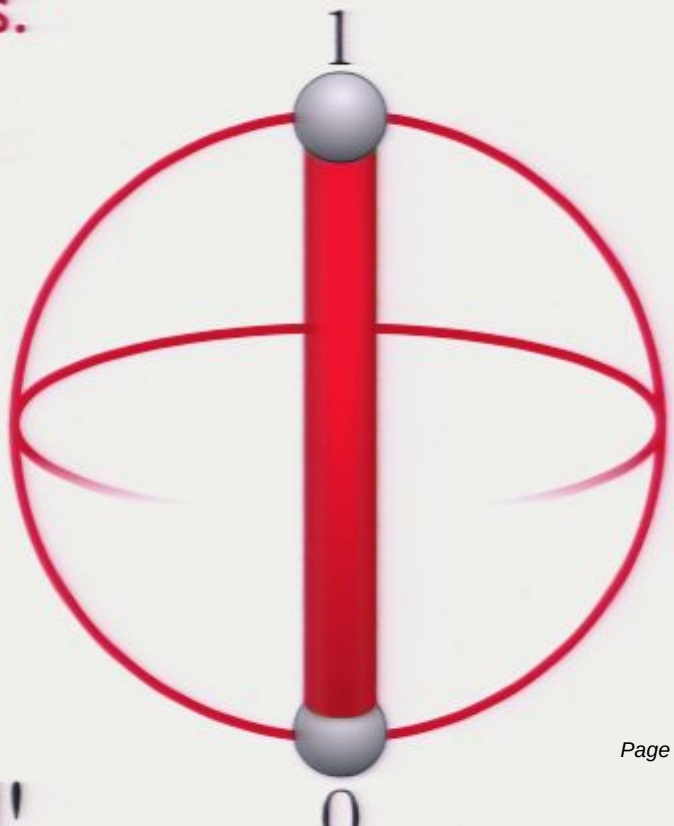
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...
- ...and even more to go from 0 back to 1...
- ...and we end up with QM!



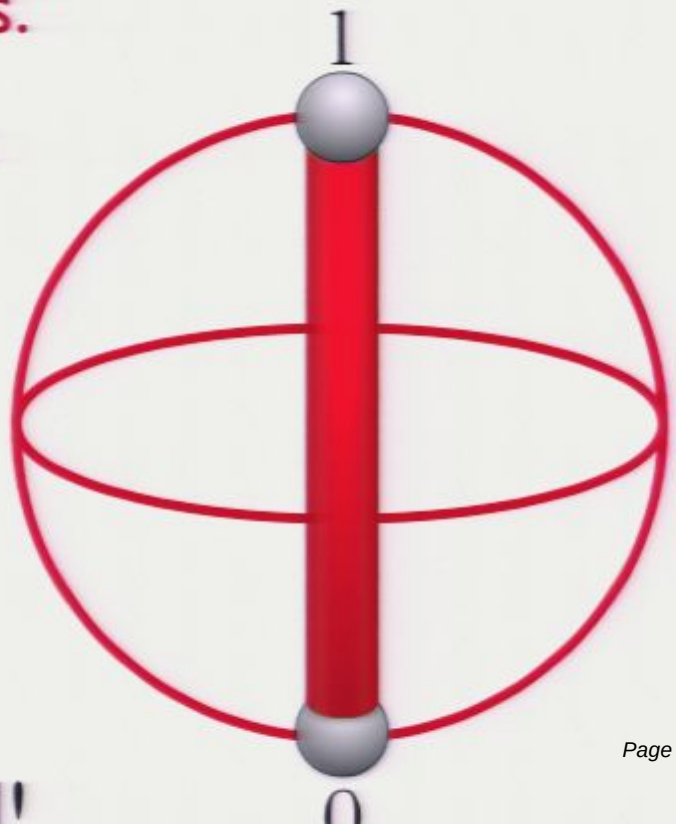
Hardy's Axiom

- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...
- ...and even more to go from 0 back to 1...
- ...and we end up with QM!



Hardy's Axiom

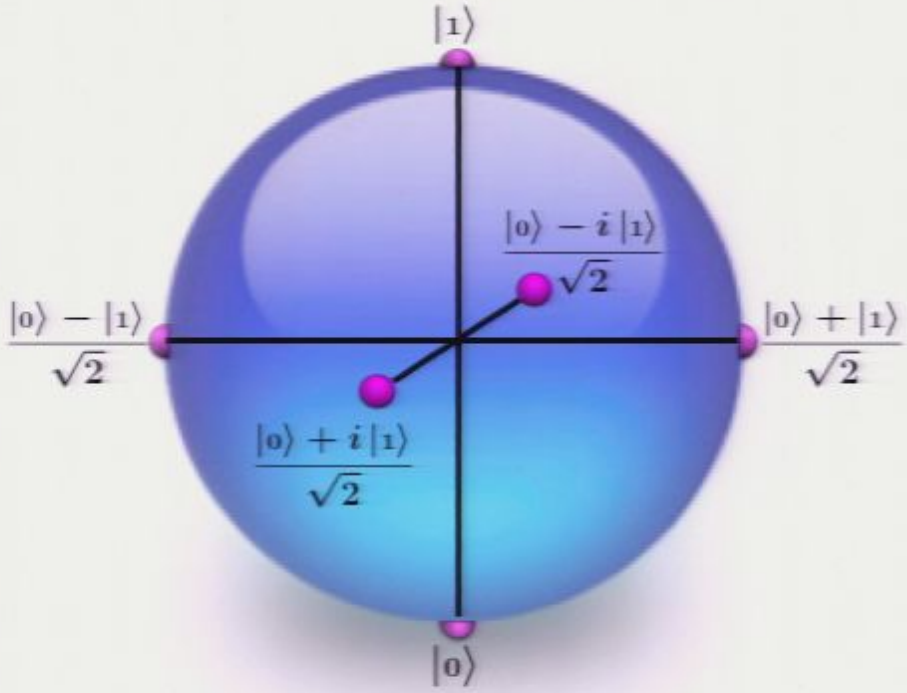
- A new demand: "There must be *continuous* and *reversible* dynamical transformations between any pair of states."
- Our probabilistic bit doesn't have enough intermediate states to go from 1 to 0!
- Need more states...
- ...and even more to go from 0 back to 1...
- ...and we end up with QM!



Quantum States

Classical Bit (Probabilistic)

Quantum Bit & the Bloch Sphere



State predicts outcome of measurements.

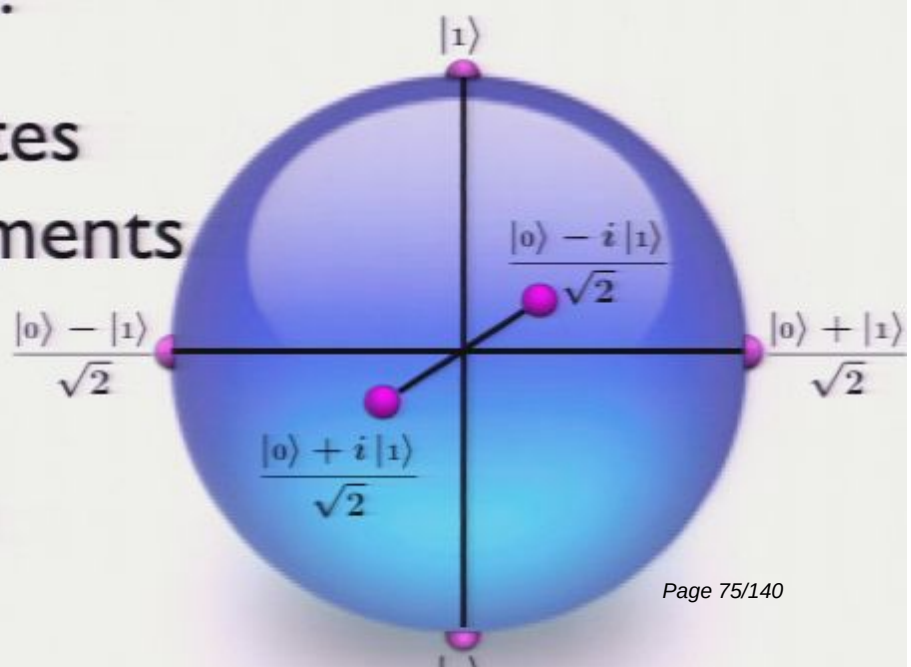
Vector space: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Longrightarrow |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

Quantum Measurements

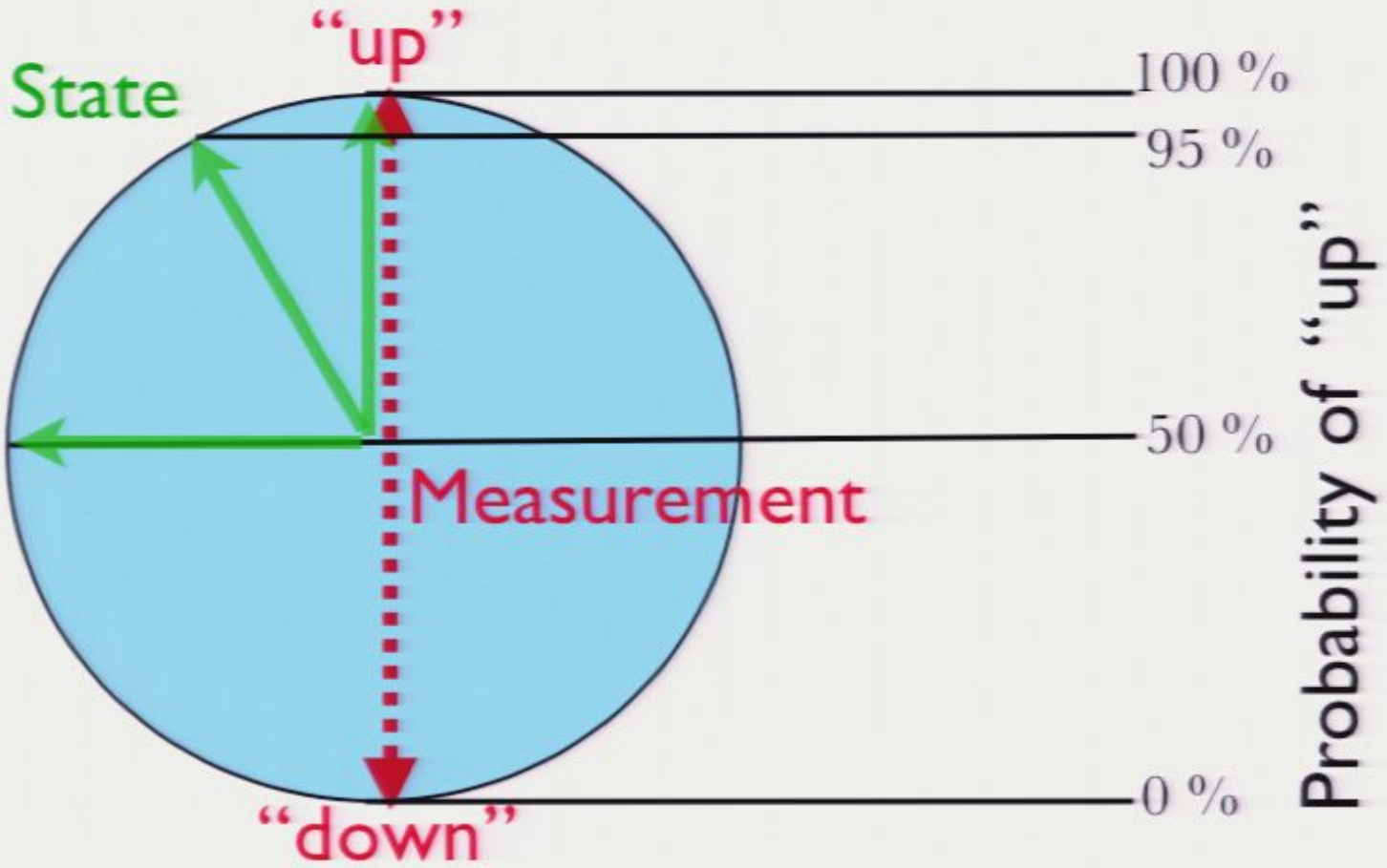
- Sole purpose of a state is *to predict the outcome of measurements*.
- Classical bit ⇒ one measurement:

  "Is the switch **on**, or **off**?"

- Quantum bit has more states
  ⇒ must be more measurements
- Symmetry implies
  each axis ⇔ measurement



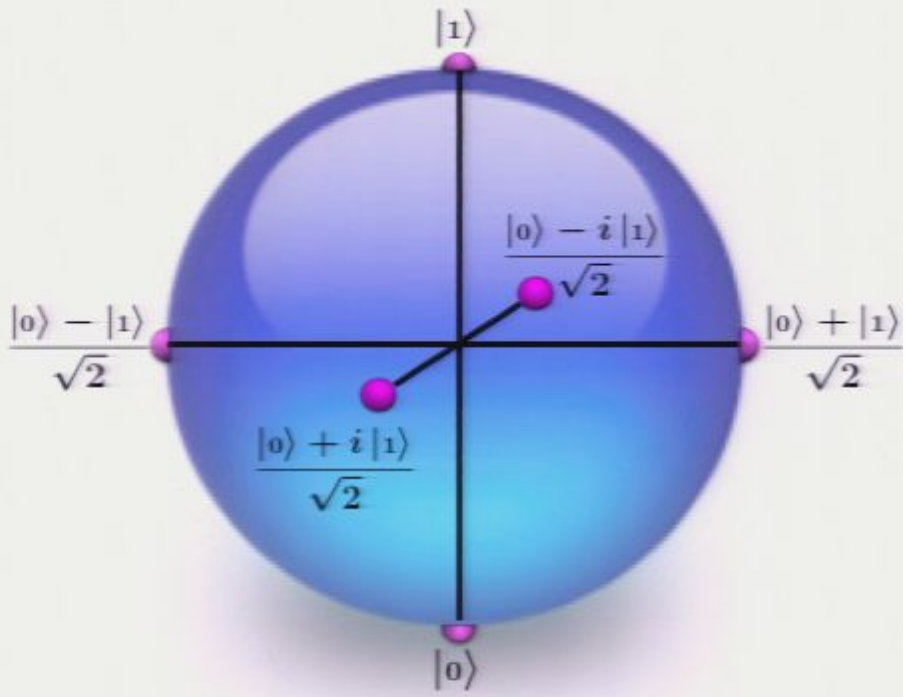
Quantum Measurements



Application: Quantum Crypto

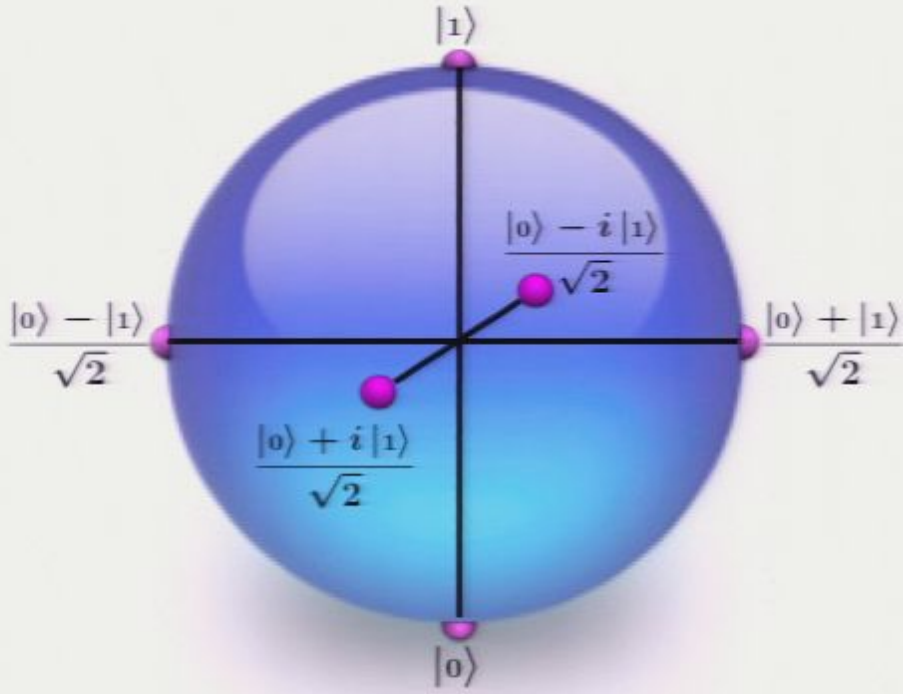
Application: Quantum Crypto

Application: Quantum Crypto



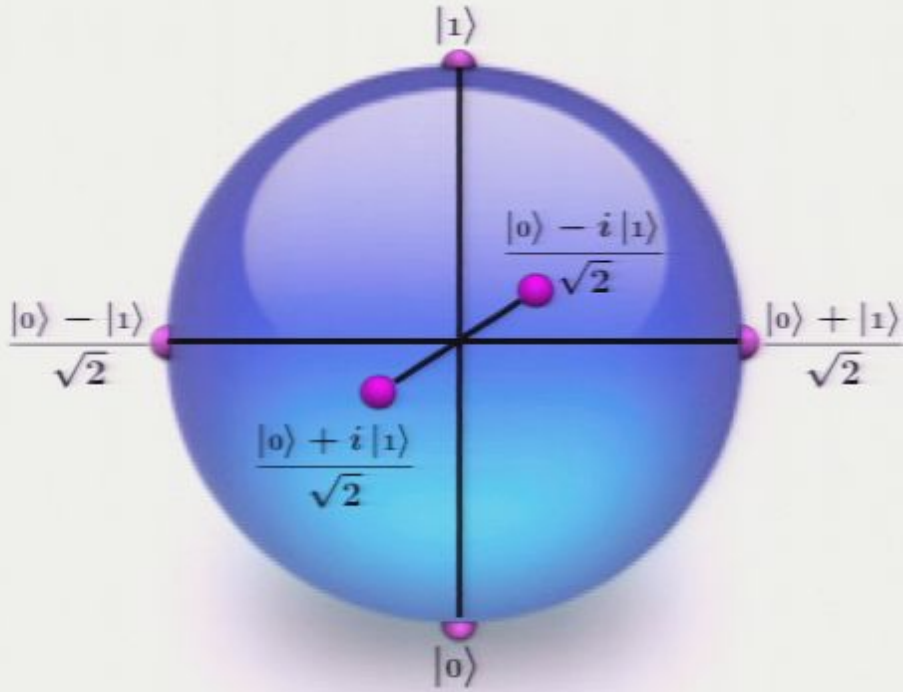
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}



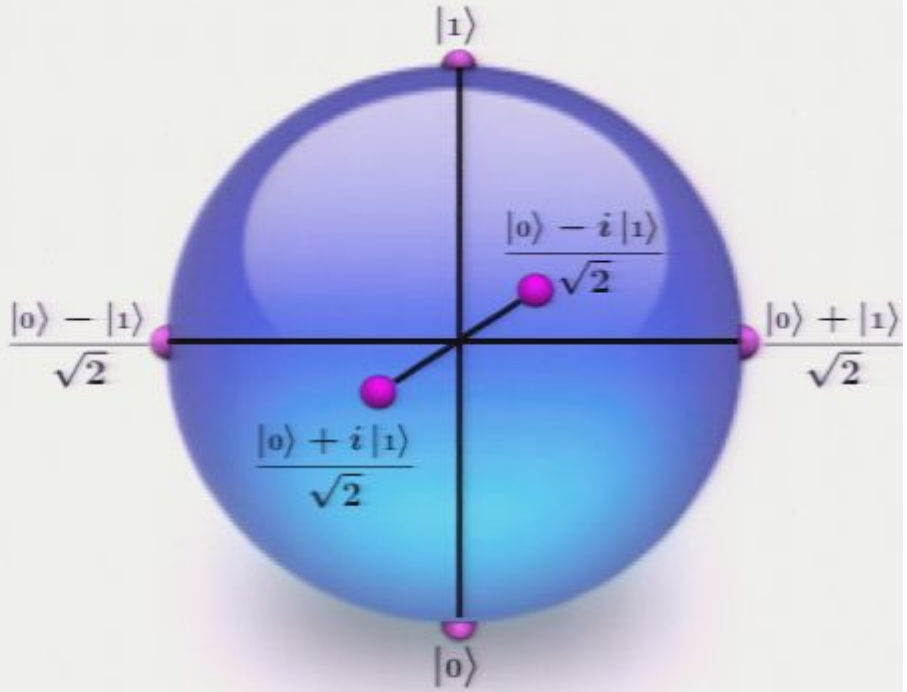
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}
- Then she sends up/left/in for "0"
  or down/right/out to indicate "1".



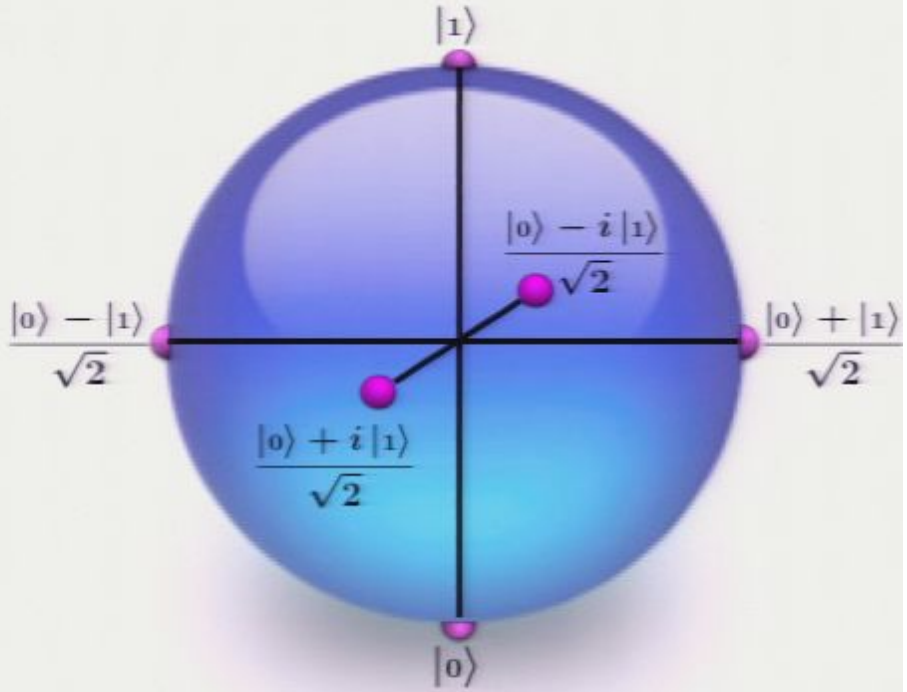
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}
- Then she sends up/left/in for "0" or down/right/out to indicate "1".
- Bob also picks a random basis, and measures it. 1/3 of the time, he gets lucky!



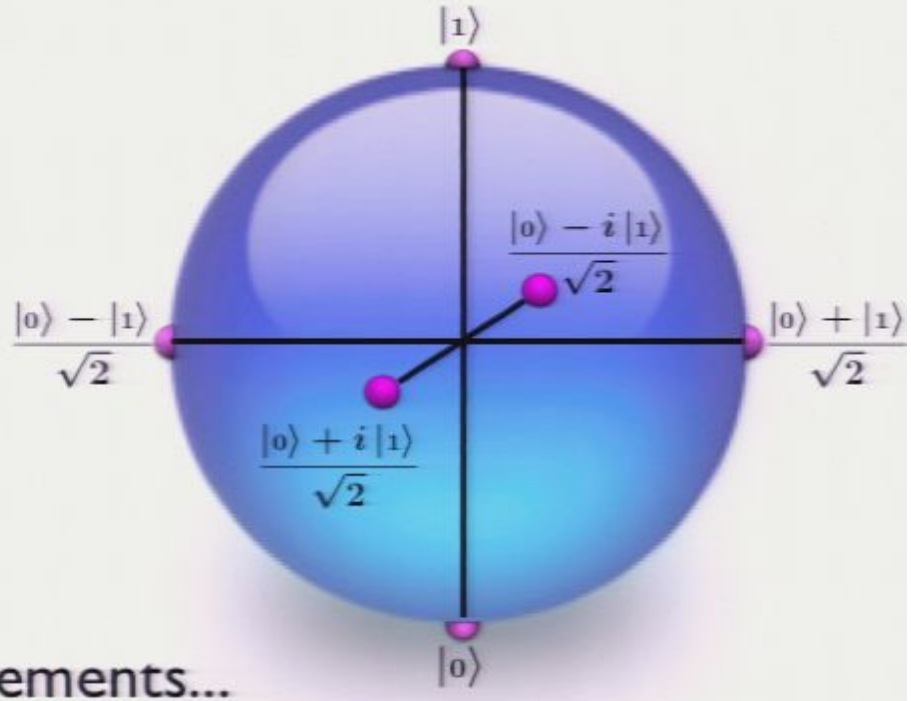
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}
- Then she sends up/left/in for "0" or down/right/out to indicate "1".
- Bob also picks a random basis, and measures it. 1/3 of the time, he gets lucky!
- **Afterward**, Alice tells Bob what basis she sent the information in.



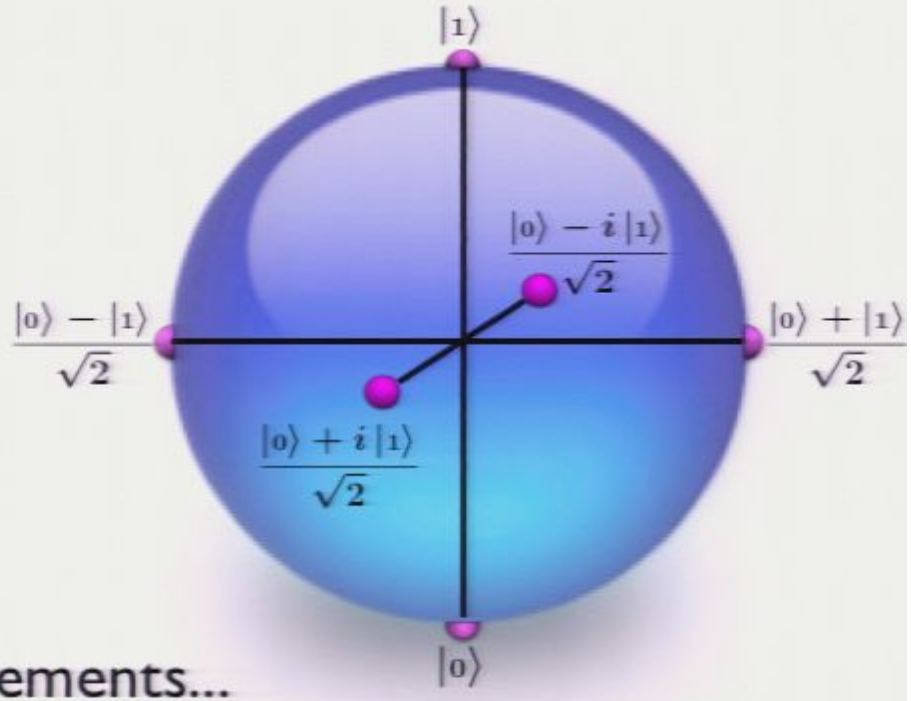
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}
- Then she sends up/left/in for "0" or down/right/out to indicate "1".
- Bob also picks a random basis, and measures it. 1/3 of the time, he gets lucky!
- **Afterward**, Alice tells Bob what basis she sent the information in.
- Bob throws away 2/3 of his measurements... ...and the remaining 1/3 agree with what Alice sent!



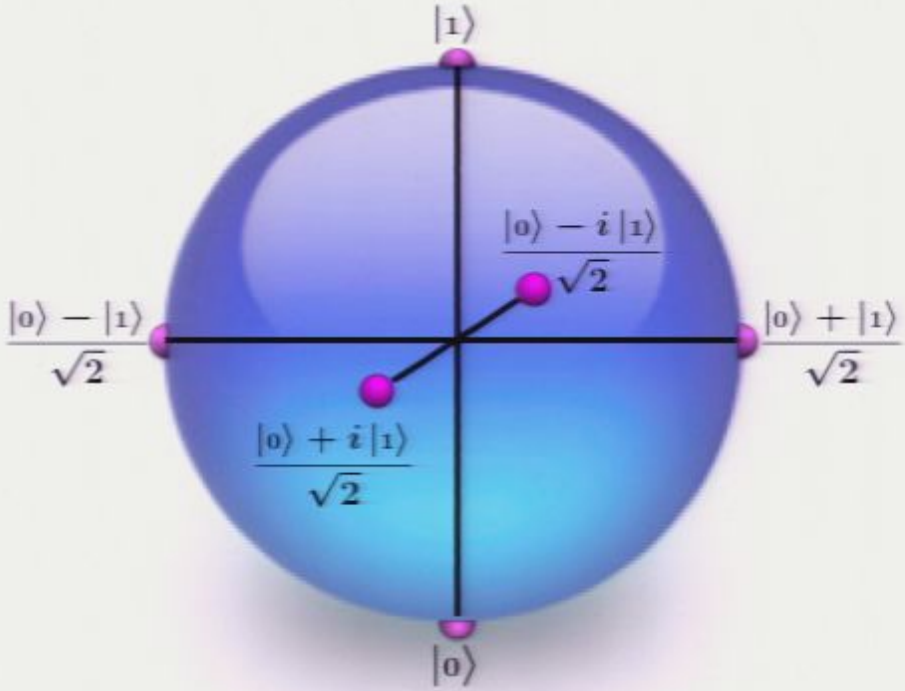
Application: Quantum Crypto

- Alice picks a random basis: {up,down} *or* {left,right} *or* {in,out}
- Then she sends up/left/in for "0" or down/right/out to indicate "1".
- Bob also picks a random basis, and measures it. 1/3 of the time, he gets lucky!
- **Afterward**, Alice tells Bob what basis she sent the information in.



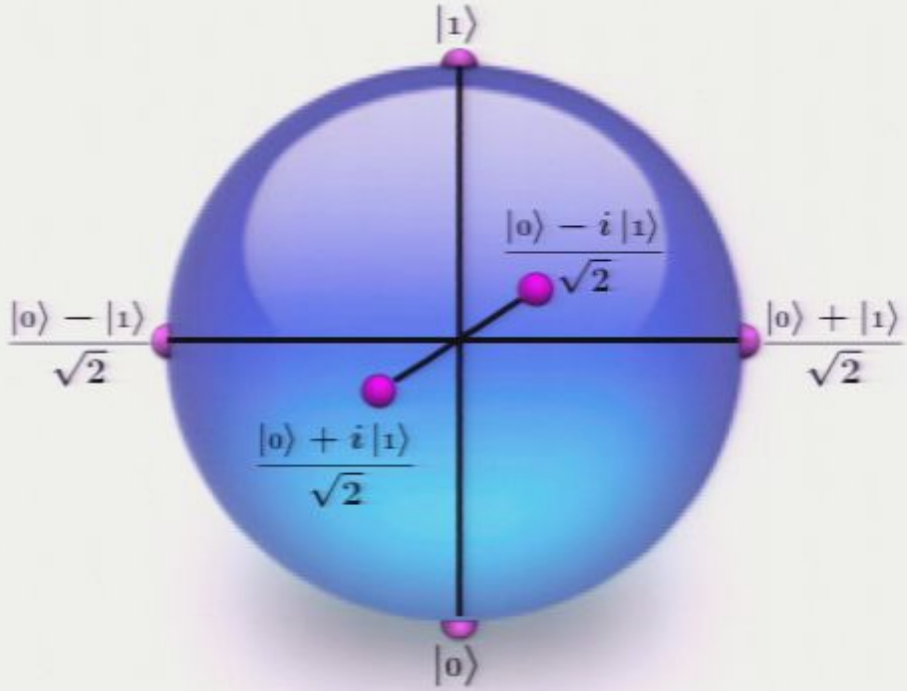
- Bob throws away 2/3 of his measurements... ...and the remaining 1/3 agree with what Alice sent!
- If an Eavesdropper listens in, she *disturbs* the qubits... which Alice and Bob can detect by comparing some of their good bits.

Quantum Dynamics (for 1 qubit!)



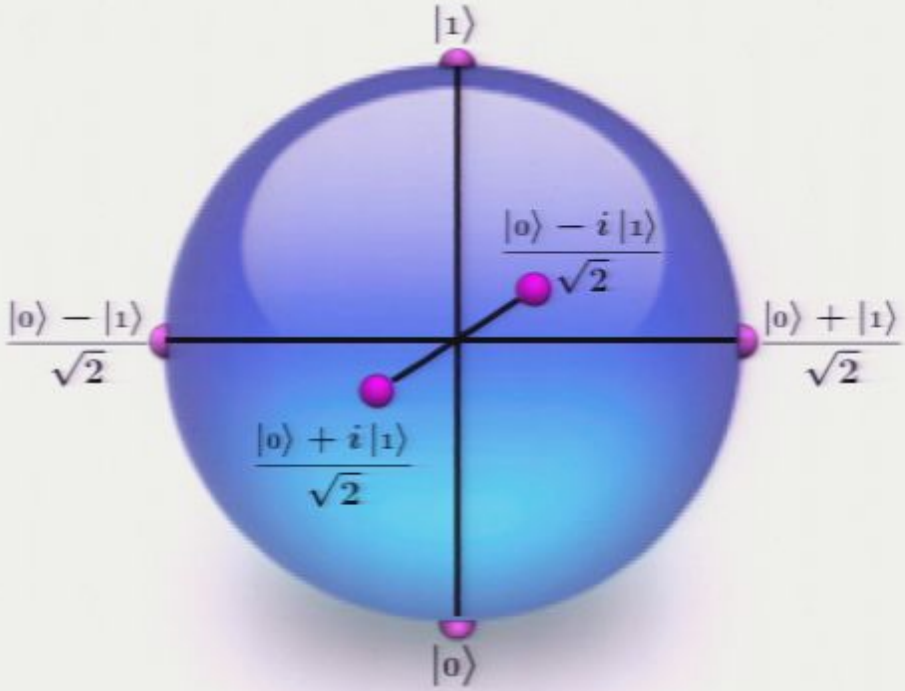
Quantum Dynamics (for 1 qubit!)

- Sphere of quantum states can rotate around any axis.



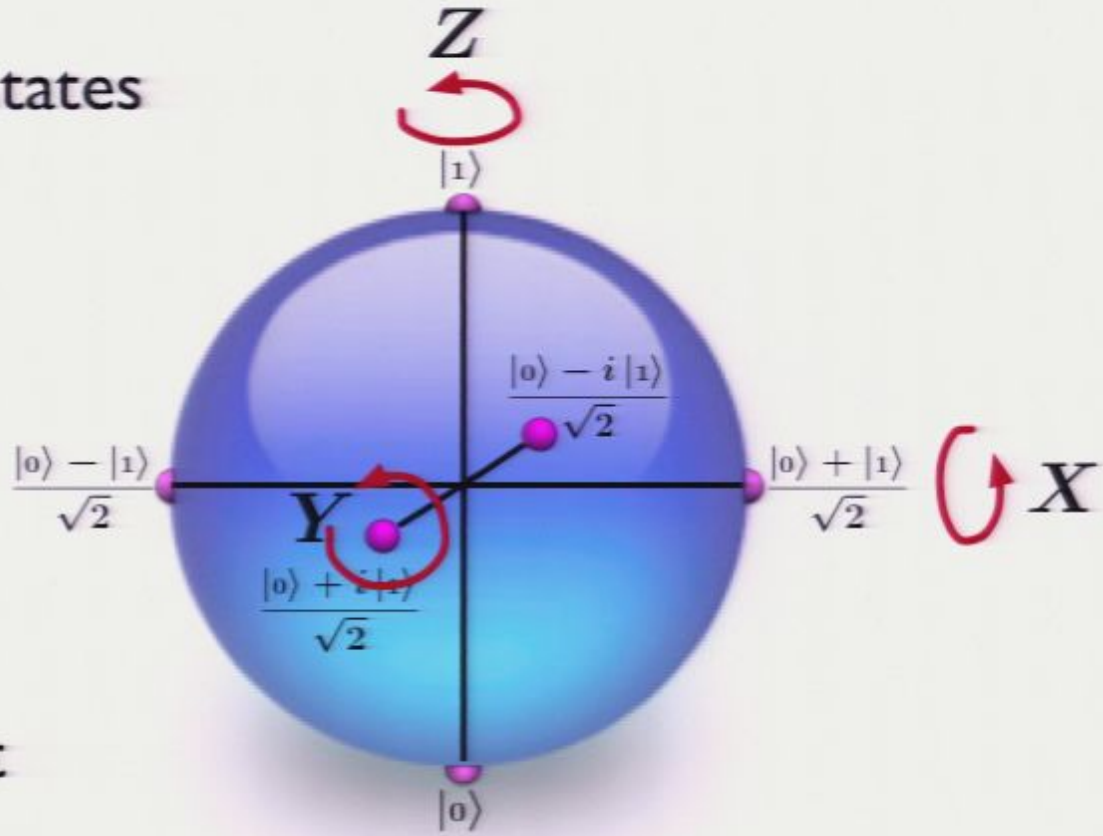
Quantum Dynamics (for 1 qubit!)

- Sphere of quantum states can rotate around any axis.
- For instance, around X, Y, or Z!



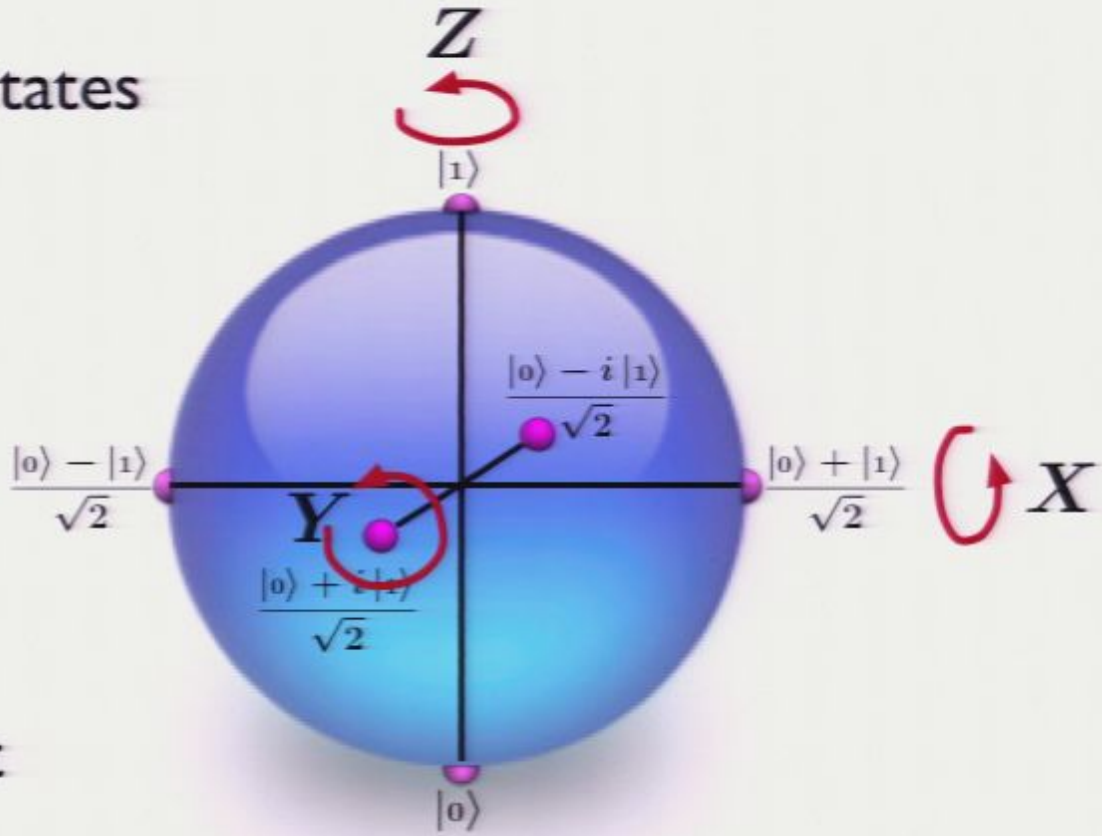
Quantum Dynamics (for 1 qubit!)

- Sphere of quantum states can rotate around any axis.
- For instance, around X, Y, or Z!
- Rotations around X, Y, and Z by 90° form the single-qubit ***Clifford Group***.



Quantum Dynamics (for 1 qubit!)

- Sphere of quantum states can rotate around any axis.
- For instance, around X, Y, or Z!
- Rotations around X, Y, and Z by 90° form the single-qubit ***Clifford Group***.

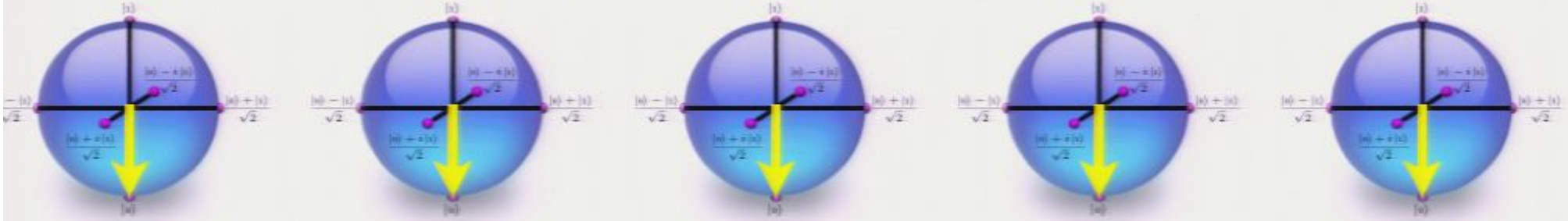


- There is a nice theorem about the Clifford group on systems of one **or** many qubits together...

Example: Gottesman-Knill Theorem

Example: Gottesman-Knill Theorem

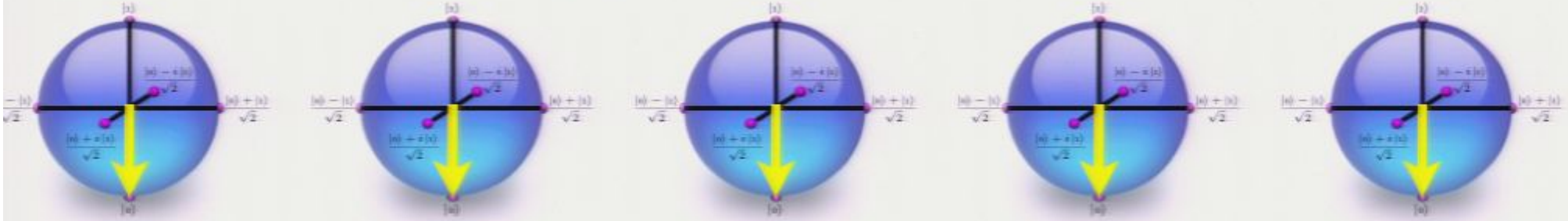
- Suppose we start with *N* qubits, each in the $|0\rangle$ state.



- ...and we do a bunch of dynamical transformations from the Clifford group...

Example: Gottesman-Knill Theorem

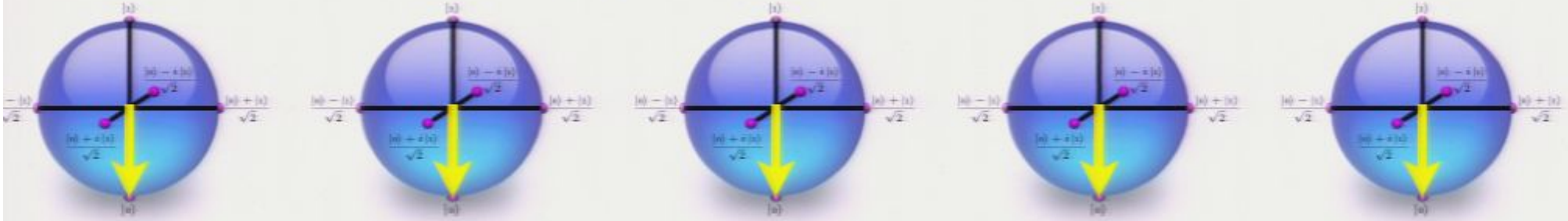
- Suppose we start with *N* qubits, each in the $|0\rangle$ state.



- ...and we do a bunch of dynamical transformations from the Clifford group...
- ...then the whole thing can be **efficiently simulated** by a classical computer!

Example: Gottesman-Knill Theorem

- Suppose we start with *N* qubits, each in the $|0\rangle$ state.



- ...and we do a bunch of dynamical transformations from the Clifford group...
- ...then the whole thing can be **efficiently simulated** by a classical computer!

...but why is this remarkable?...

Quantum Computation

- In general, dynamics of large quantum systems (e.g., *N* qubits) **can't** be simulated in less than $O(2^N)$ time by a classical computer. *Why?*

Quantum Computation

- In general, dynamics of large quantum systems (e.g., N qubits) **can't** be simulated in less than $O(2^N)$ time by a classical computer. *Why?*
- Basically, *amplitudes* are much harder to track than *probabilities*, because of interference!

Quantum Computation

- In general, dynamics of large quantum systems (e.g., *N* qubits) **can't** be simulated in less than $O(2^N)$ time by a classical computer. *Why?*
- Basically, *amplitudes* are much harder to track than *probabilities*, because of interference!
- Feynman pointed out that a computer built of qubits could simulate quantum systems...

Quantum Computation

- In general, dynamics of large quantum systems (e.g., N qubits) **can't** be simulated in less than $O(2^N)$ time by a classical computer. *Why?*
- Basically, *amplitudes* are much harder to track than *probabilities*, because of interference!
- Feynman pointed out that a computer built of qubits could simulate quantum systems...
- ...so would such a device be more powerful than a classical computer?

Quantum Computer = Supercomputer???

Quantum Computer = Supercomputer???

- Quantum computer: a bunch of qubits, protected from noise, on which we can do 1- and 2-qubit *gates* (dynamical operations).

Quantum Computer = Supercomputer???

- Quantum computer: a bunch of qubits, protected from noise, on which we can do 1- and 2-qubit *gates* (dynamical operations).
- Can a QC solve hard problems quickly? YES: quantum simulation, factoring, and a few others.

  => *ironically, a QC can break RSA crypto!*

Quantum Computer = Supercomputer???

- Quantum computer: a bunch of qubits, protected from noise, on which we can do 1- and 2-qubit *gates* (dynamical operations).
- Can a QC solve hard problems quickly? YES: quantum simulation, factoring, and a few others.
  => *ironically, a QC can break RSA crypto!*
- Can a QC solve all hard problems quickly! NO.

Quantum Computer = Supercomputer???

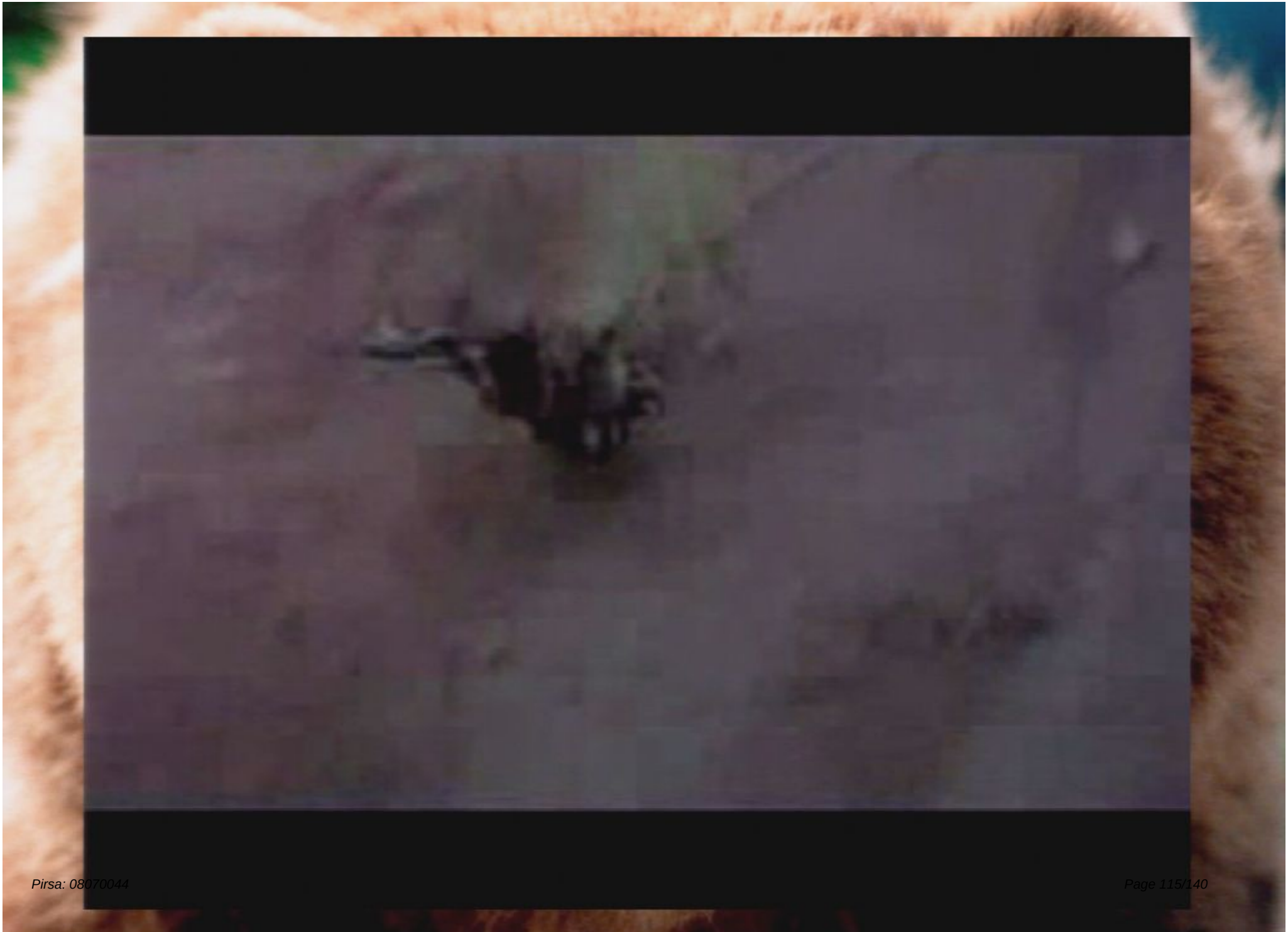
- Quantum computer: a bunch of qubits, protected from noise, on which we can do 1- and 2-qubit *gates* (dynamical operations).
- Can a QC solve hard problems quickly? YES: quantum simulation, factoring, and a few others.
  => *ironically, a QC can break RSA crypto!*
- Can a QC solve all hard problems quickly! NO.
- Will a QC run regular software really fast? NO.

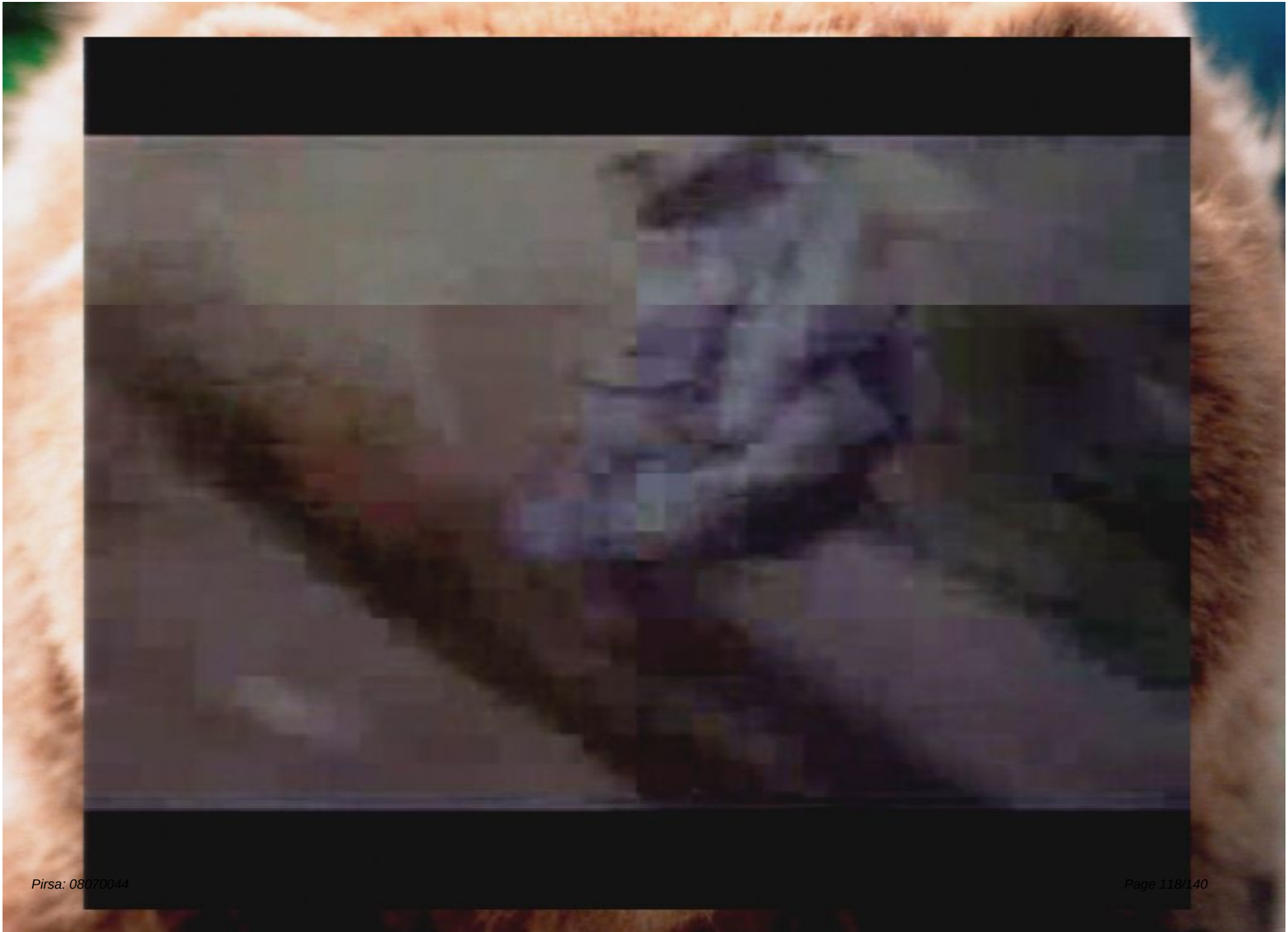

Ursus Mark IV, 1988

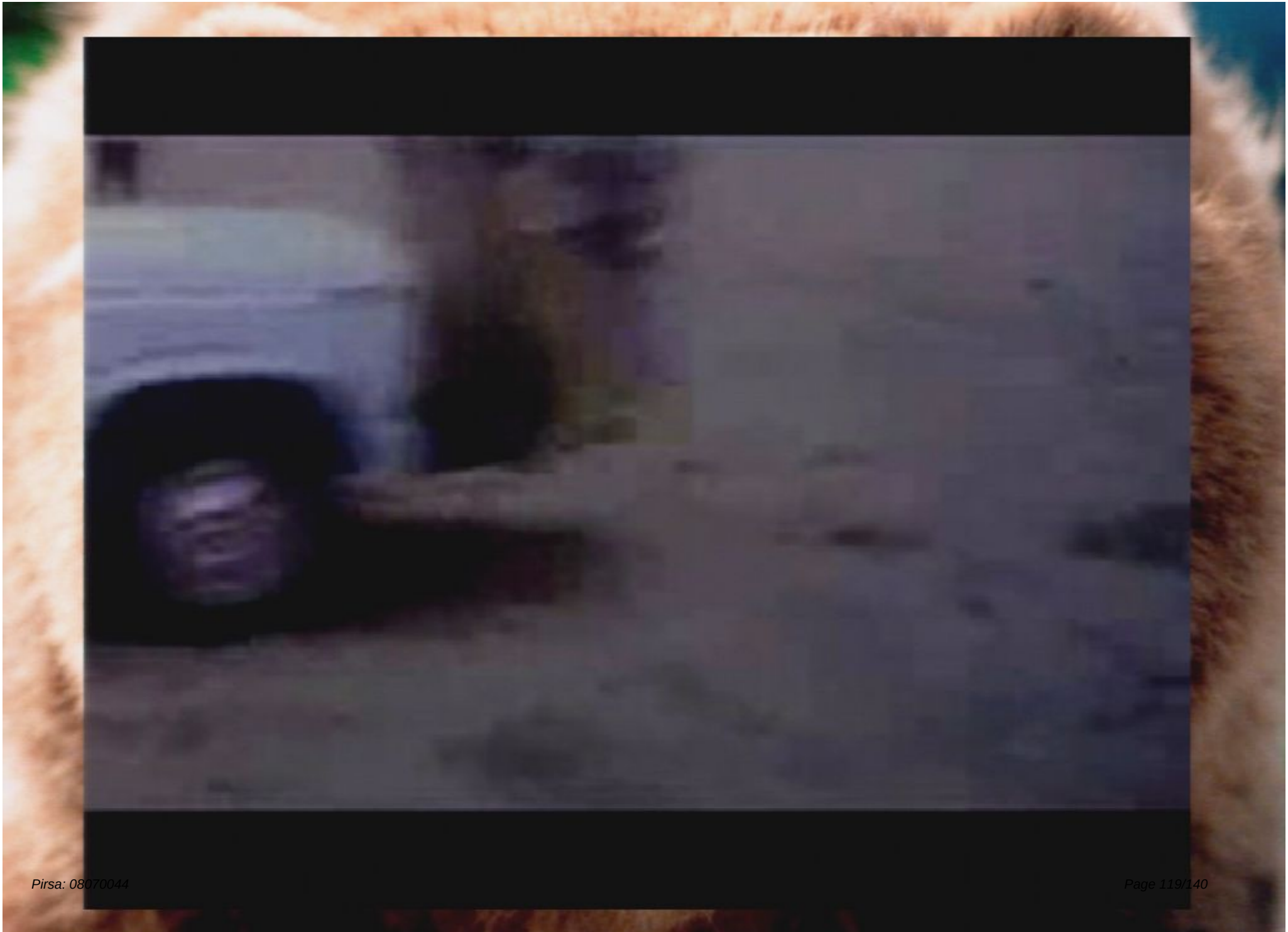

Ursus Mark IV, 1988

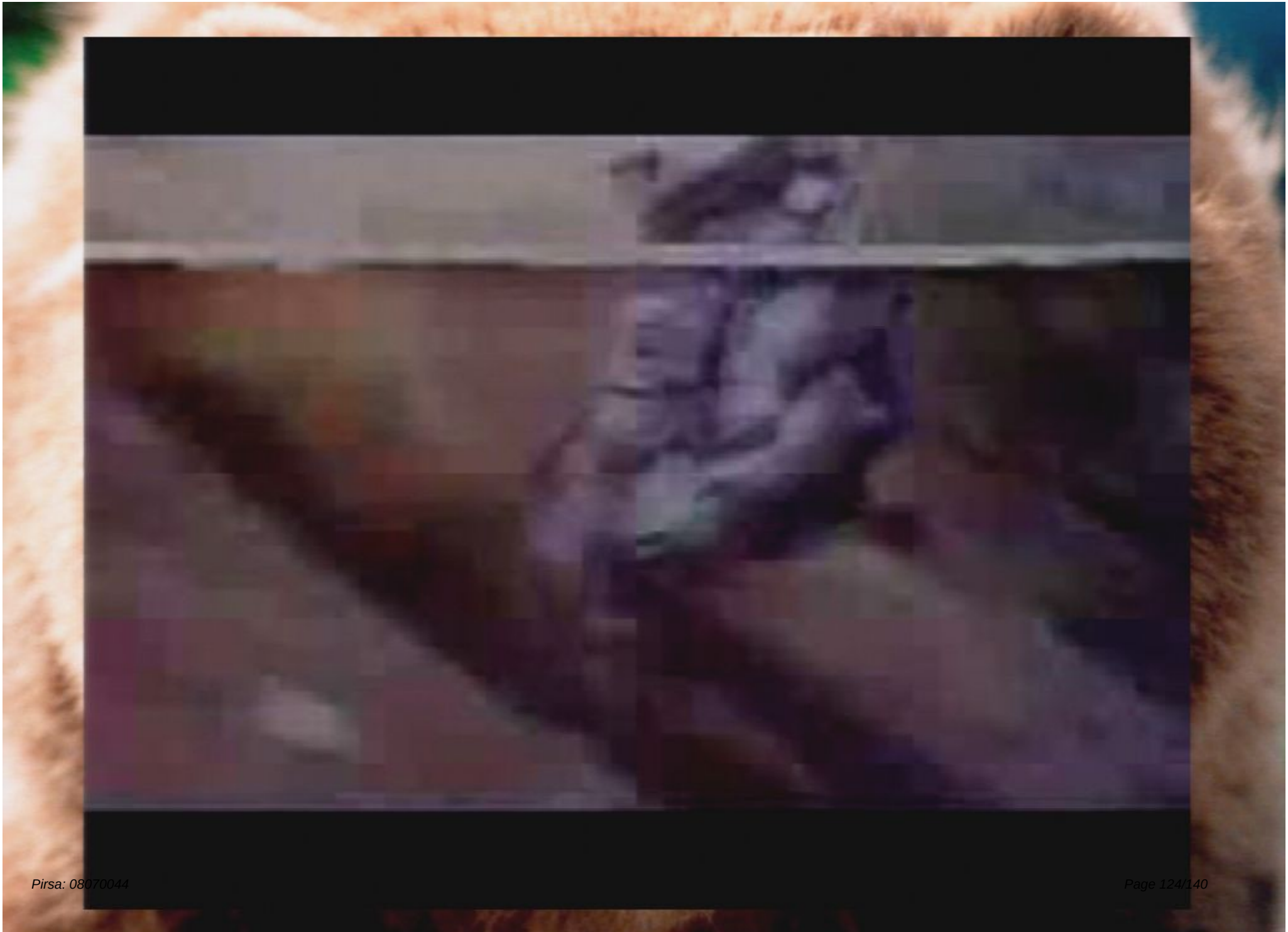

Ursus Mark V, Series A, 1989

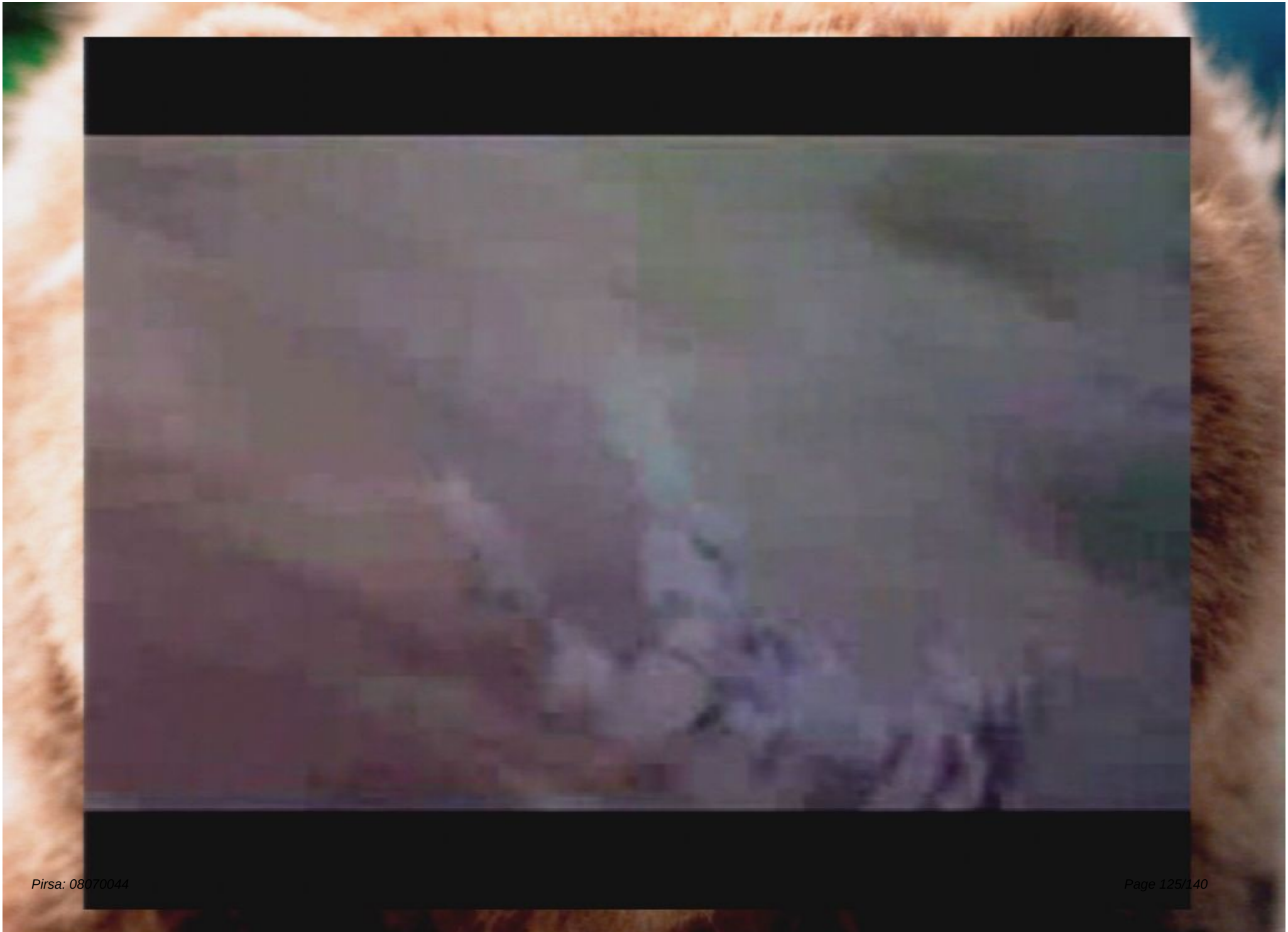

Niagara Escarpment, 1989
Hamilton, Ontario

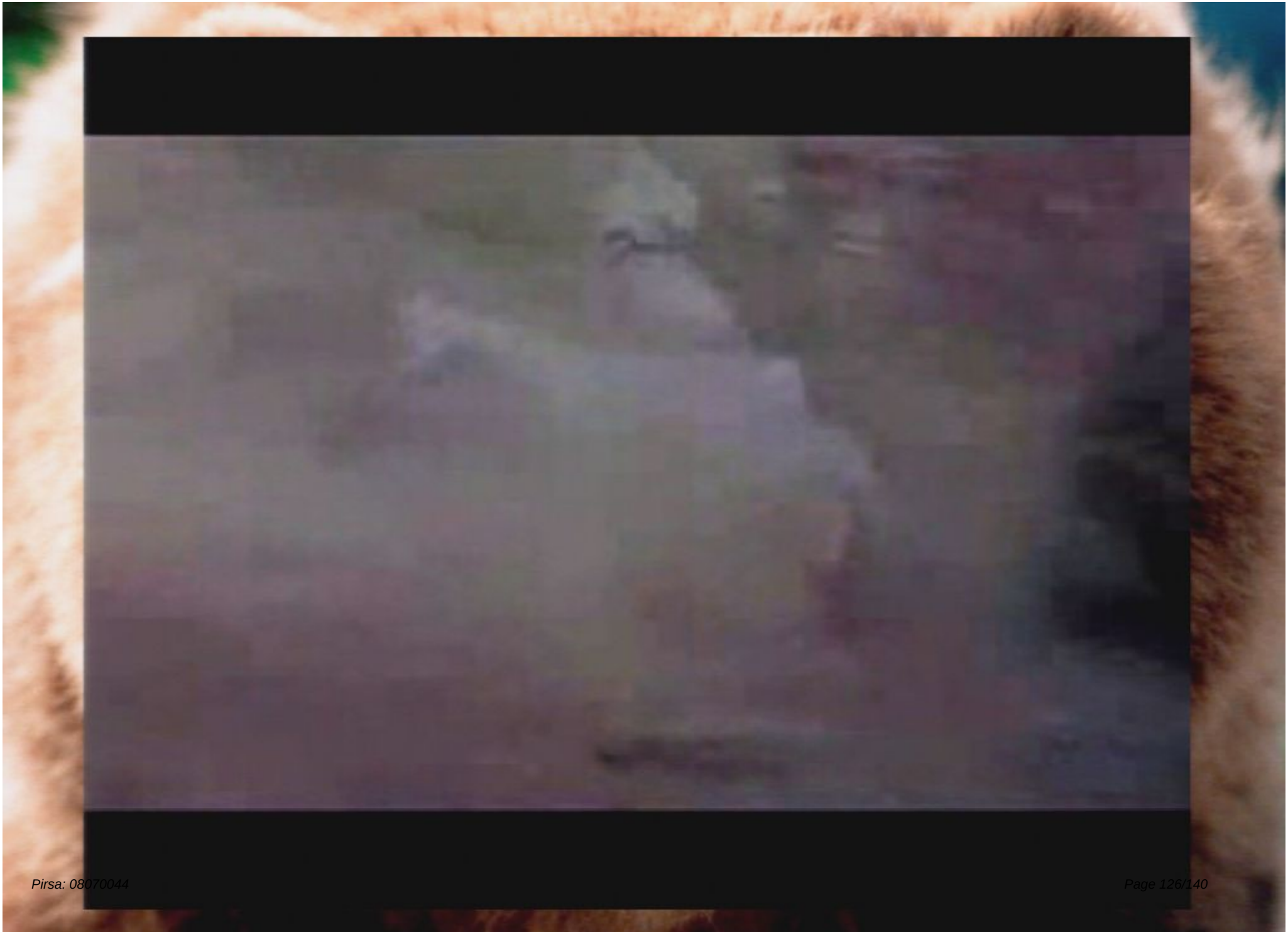


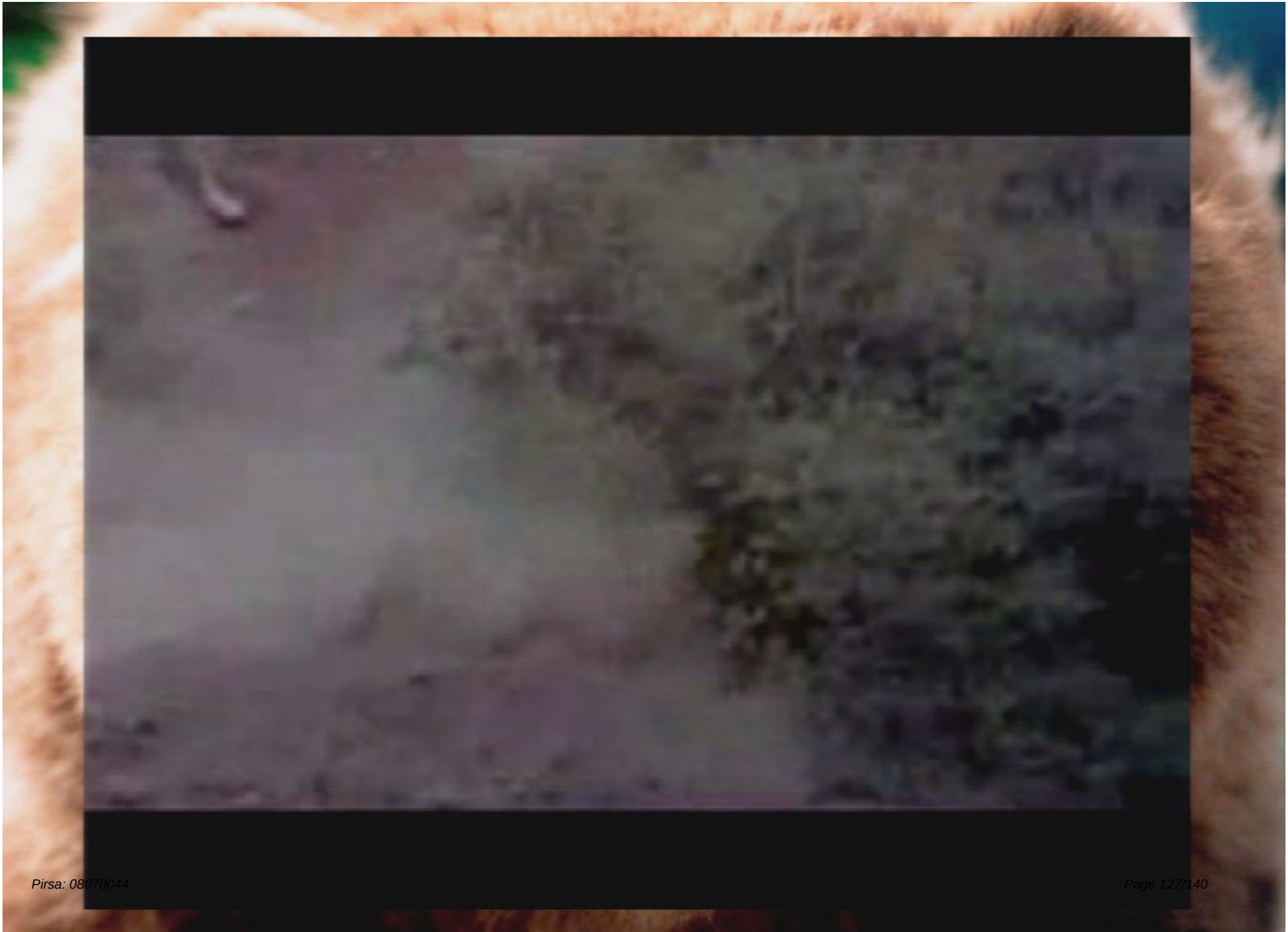








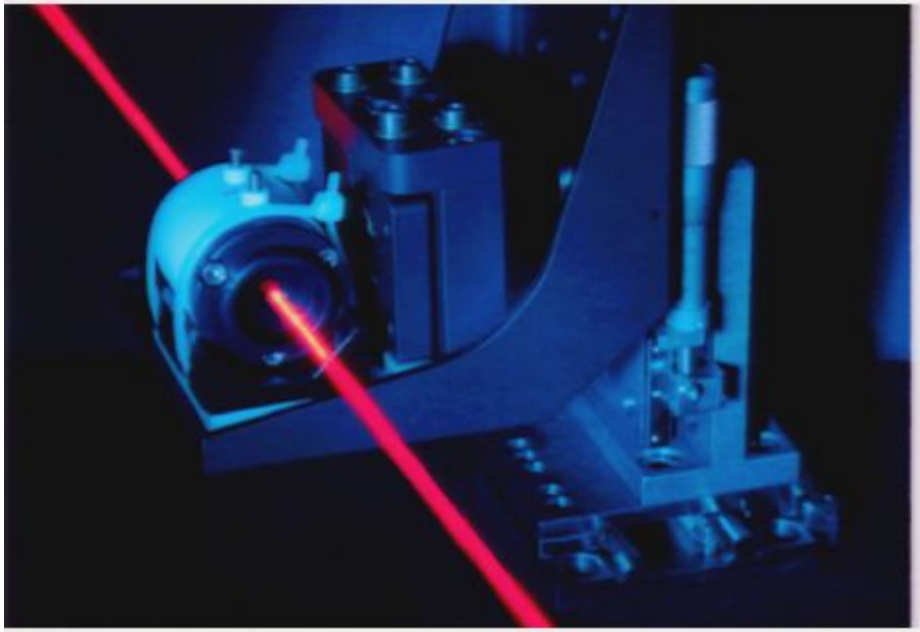


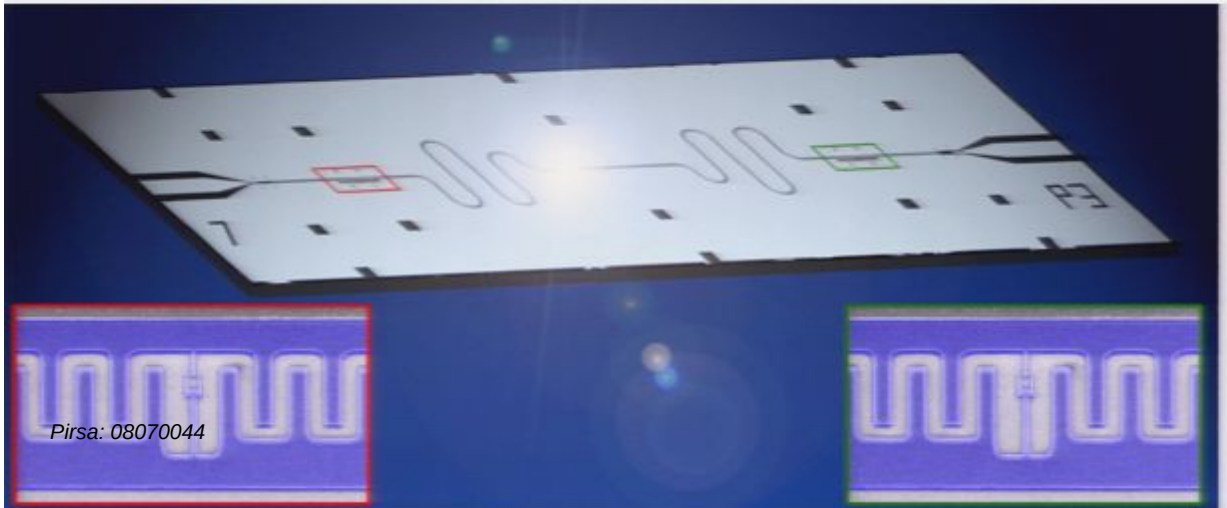


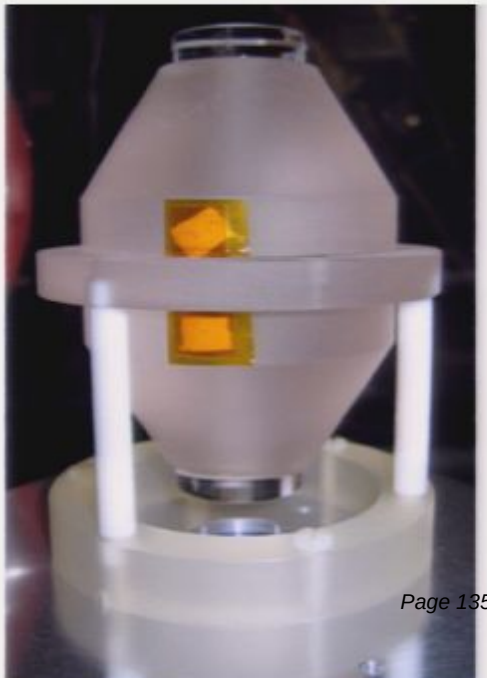
The Science:
Quantum Info in the Lab

The Science: Quantum Info in the Lab

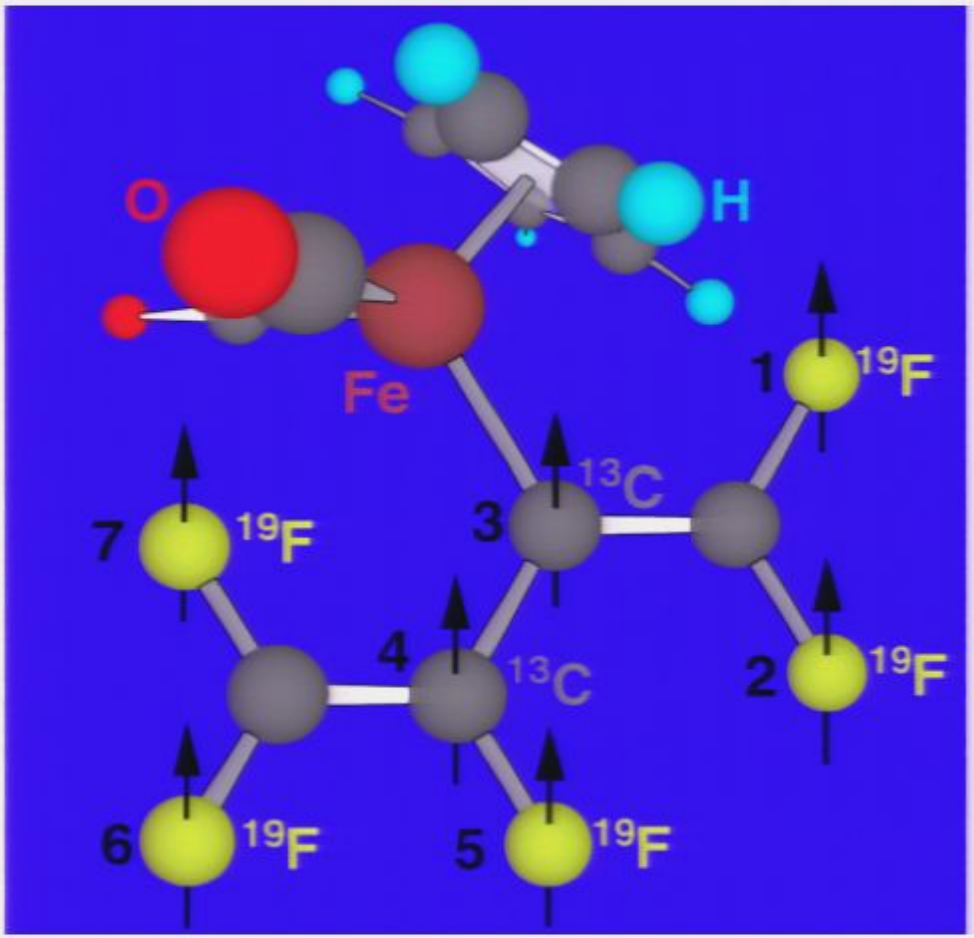
Photons: the ideal qubit





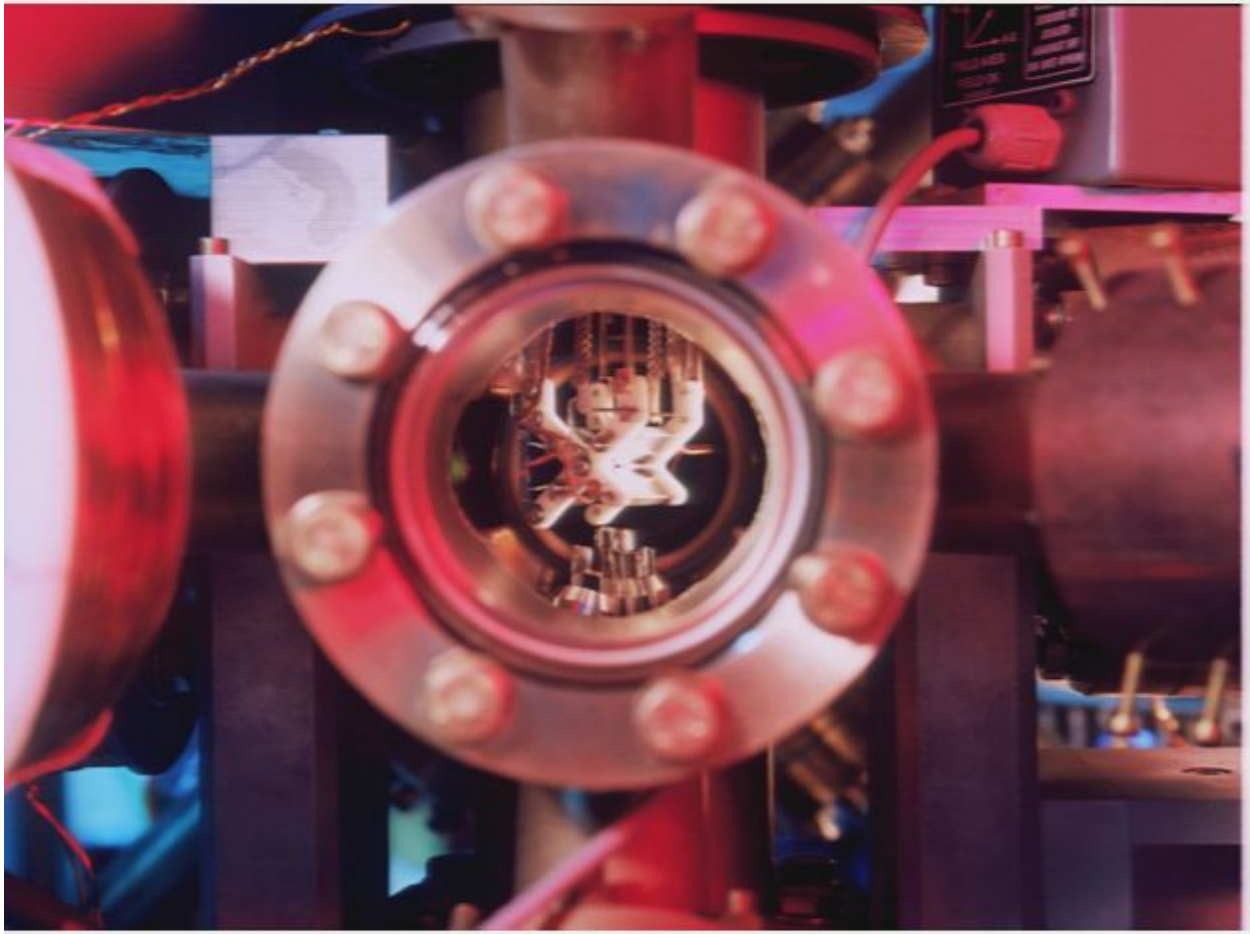


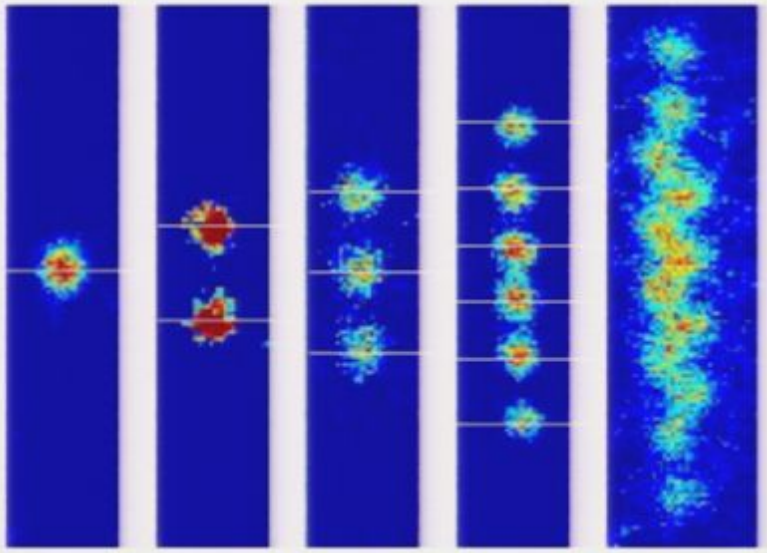
Nuclear Magnetic Resonance: here today, gone tomorrow

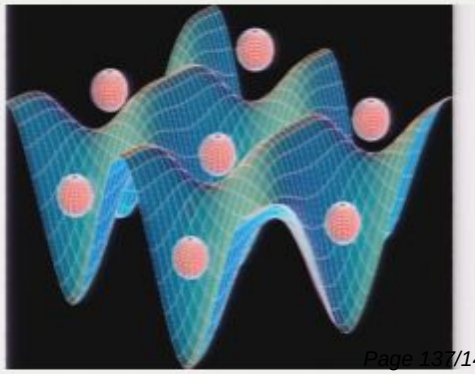


NMR QC (5-bit)

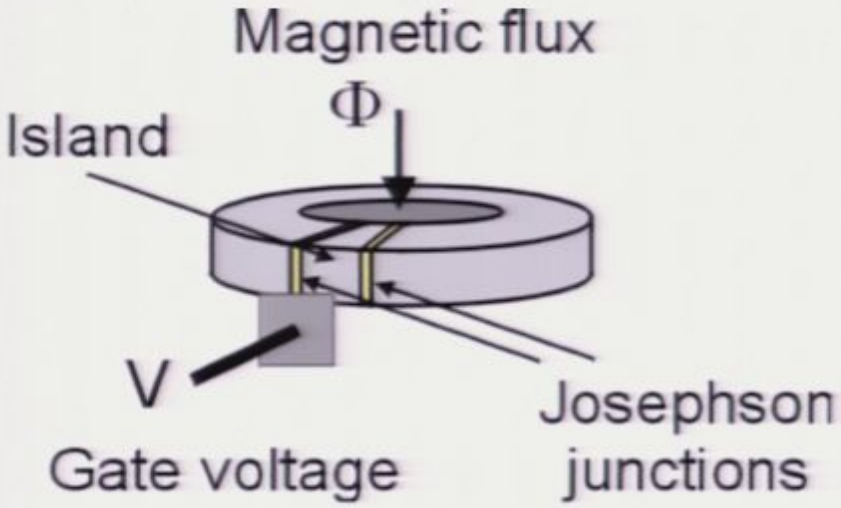
Atoms & Ions: precise control

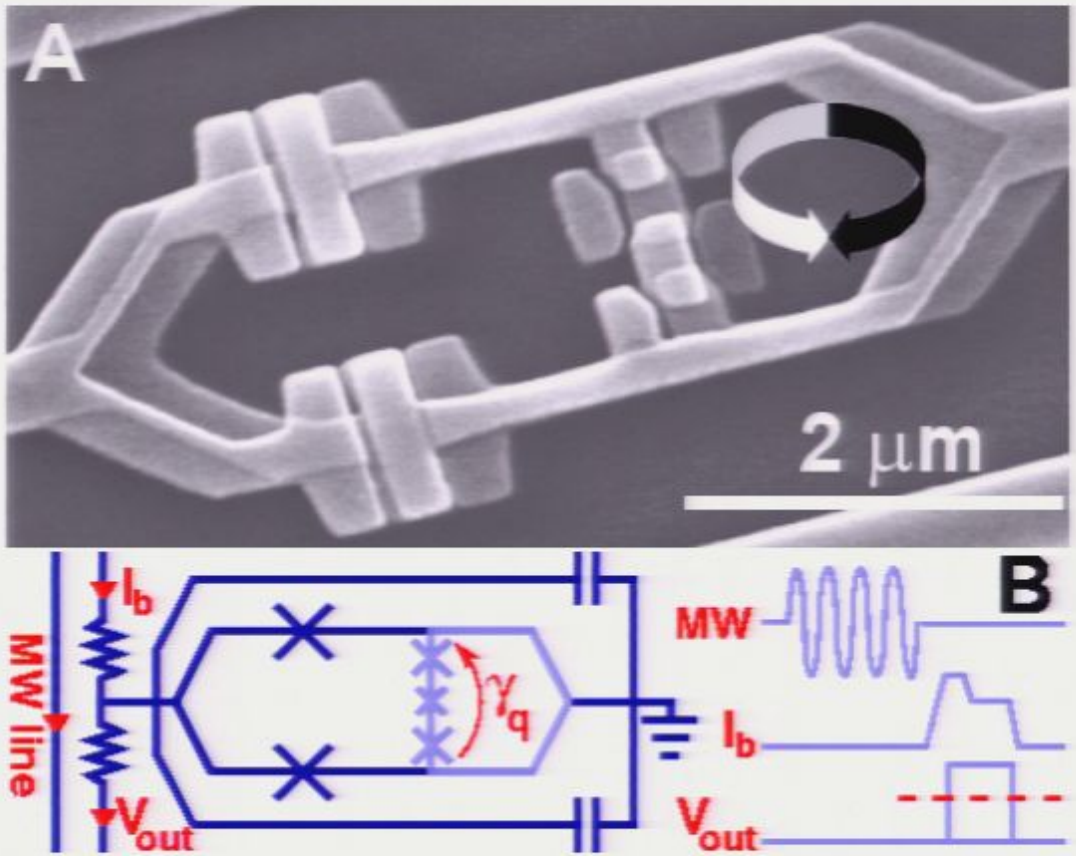






SQUIDs: technology of tomorrow?





Research Fronts

- Quantum error-correcting codes
- Fault-tolerant quantum computation
- Novel models of quantum computing
  - adiabatic QC
  - measurement-based "single-use" QC
  - topological QC
- What is QM a theory **of**? Reality? or knowledge?
- Where does the power of QC come from?
- Designing new quantum algorithms
- Decoherence: why does the world look classical?