Title: Keynote Presentation - Harnessing the Quantum World

Date: Jul 26, 2006 09:00 AM

URL: http://pirsa.org/06070073

Abstract:

Harnessing the Quantum World

Institute *for* Quantum Computing

Harnessing the Quantum World

IQC Institute *for* Quantum Computing

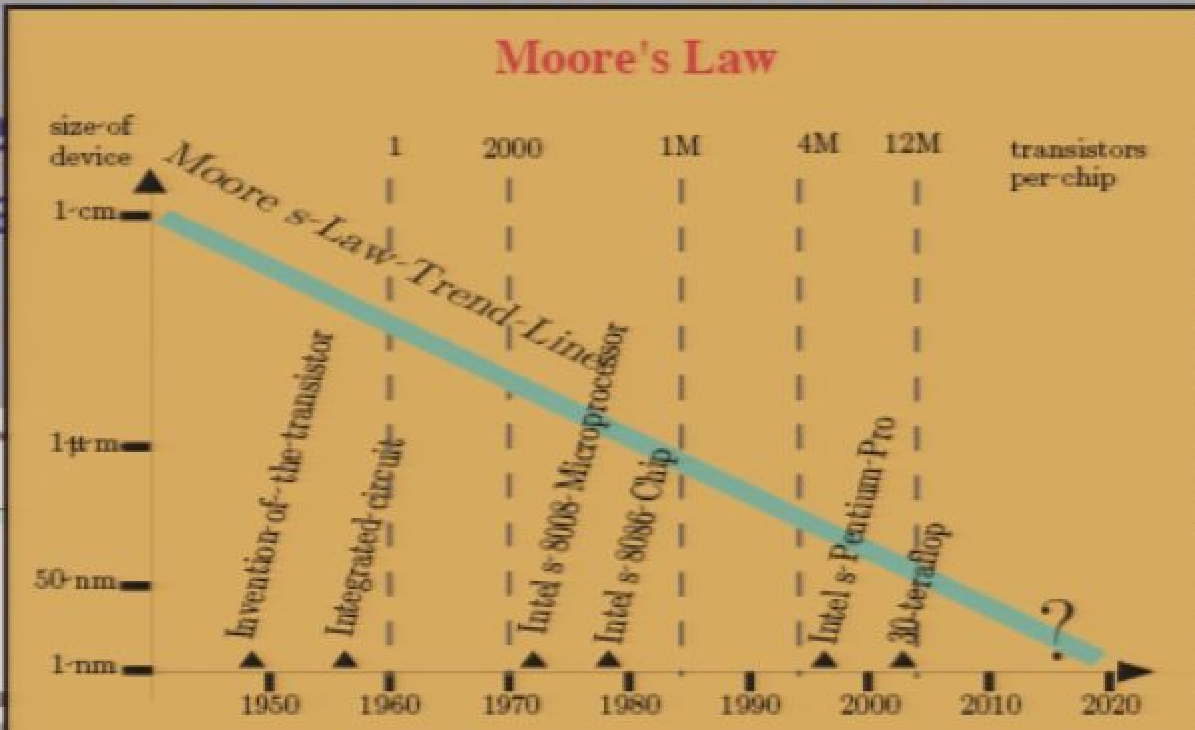
Plan

- Why quantum information?
- What is quantum computing?
- Steps towards building these devices.

Information Processing Devices

Why Quant. Info. Processing?

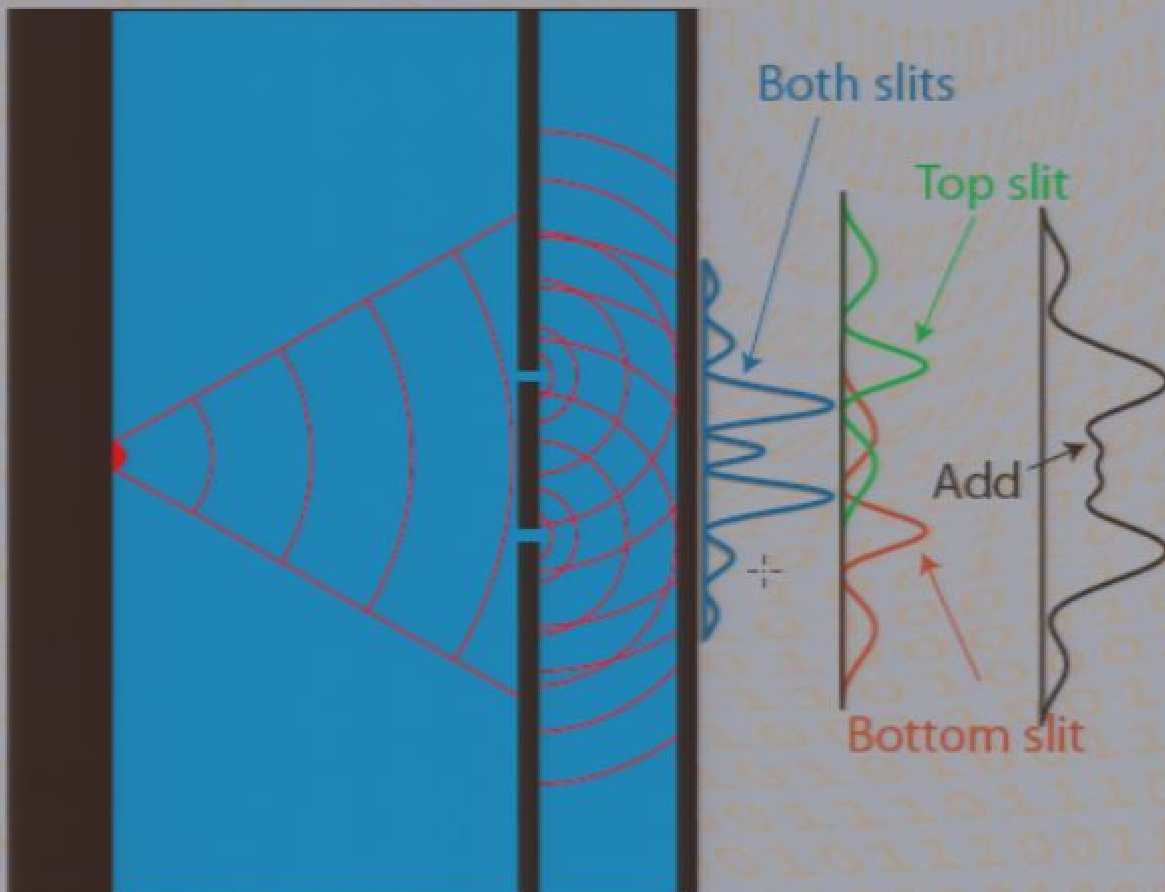
We are
the qua

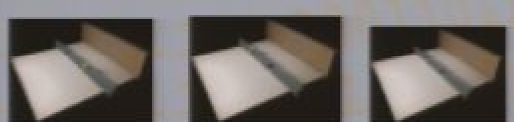


The size of transistors is decreasing rapidly, around 2020 they will be of atomic size.

Basics of Quantum Mechanics

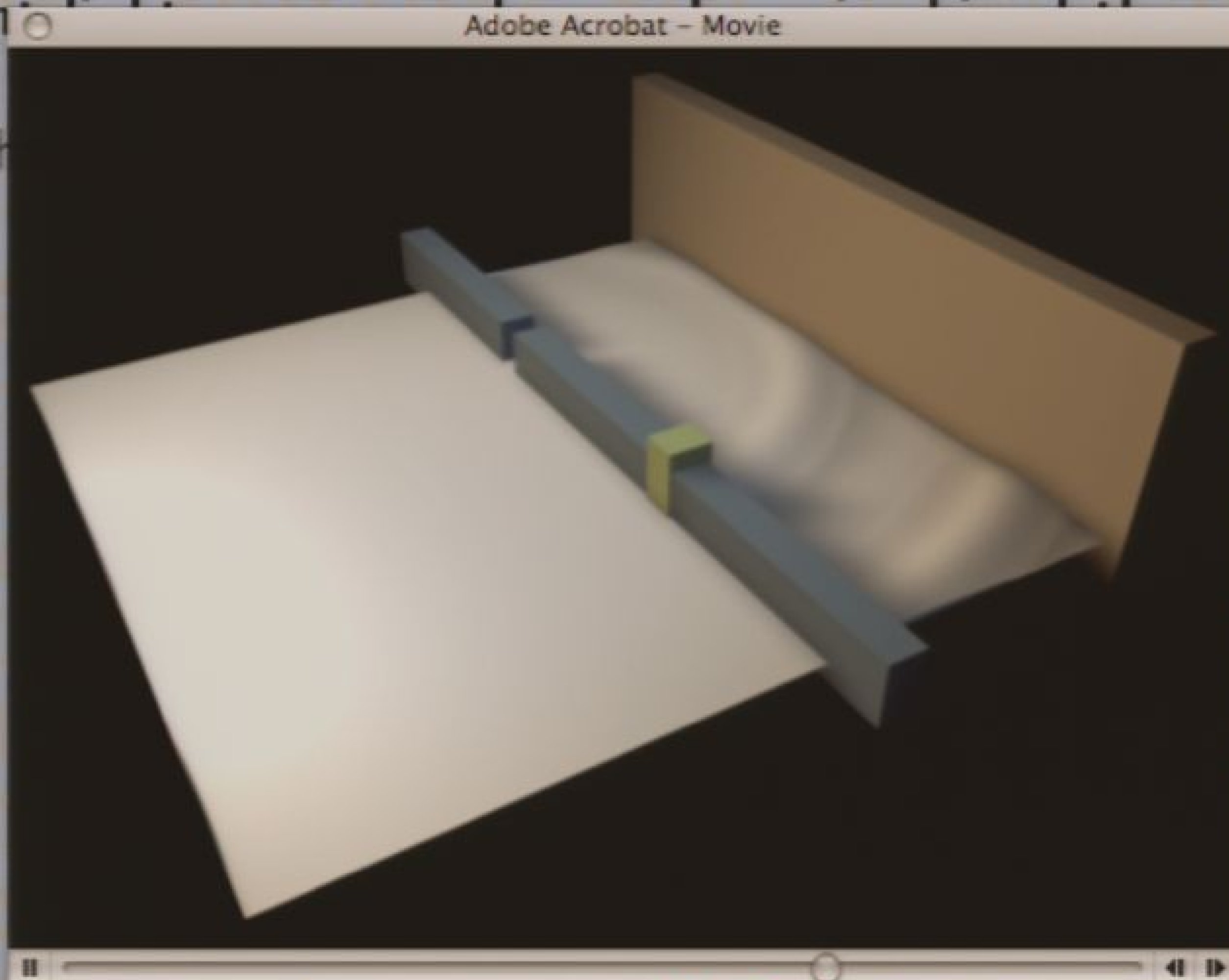
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





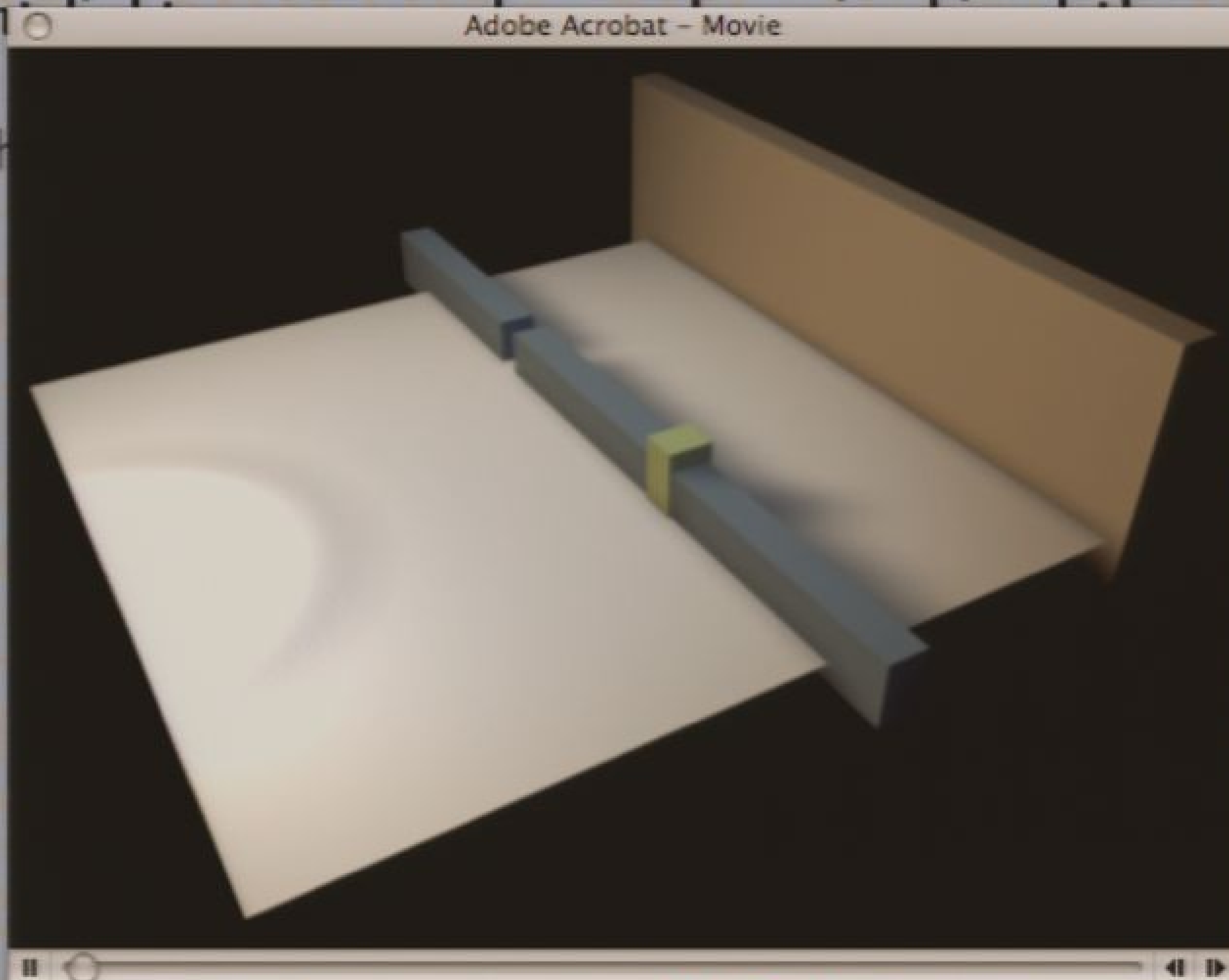
Basics of Quantum Mechanics

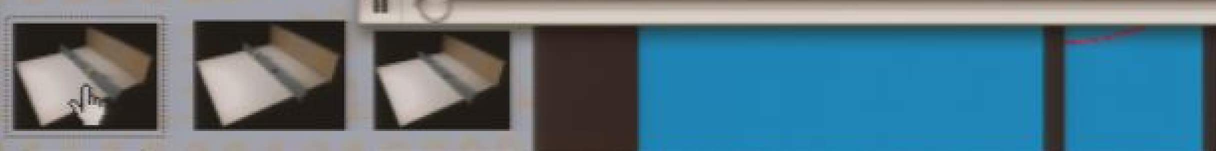
A coheren gh 2 slits,
the result final result
when both



Basics of Quantum Mechanics

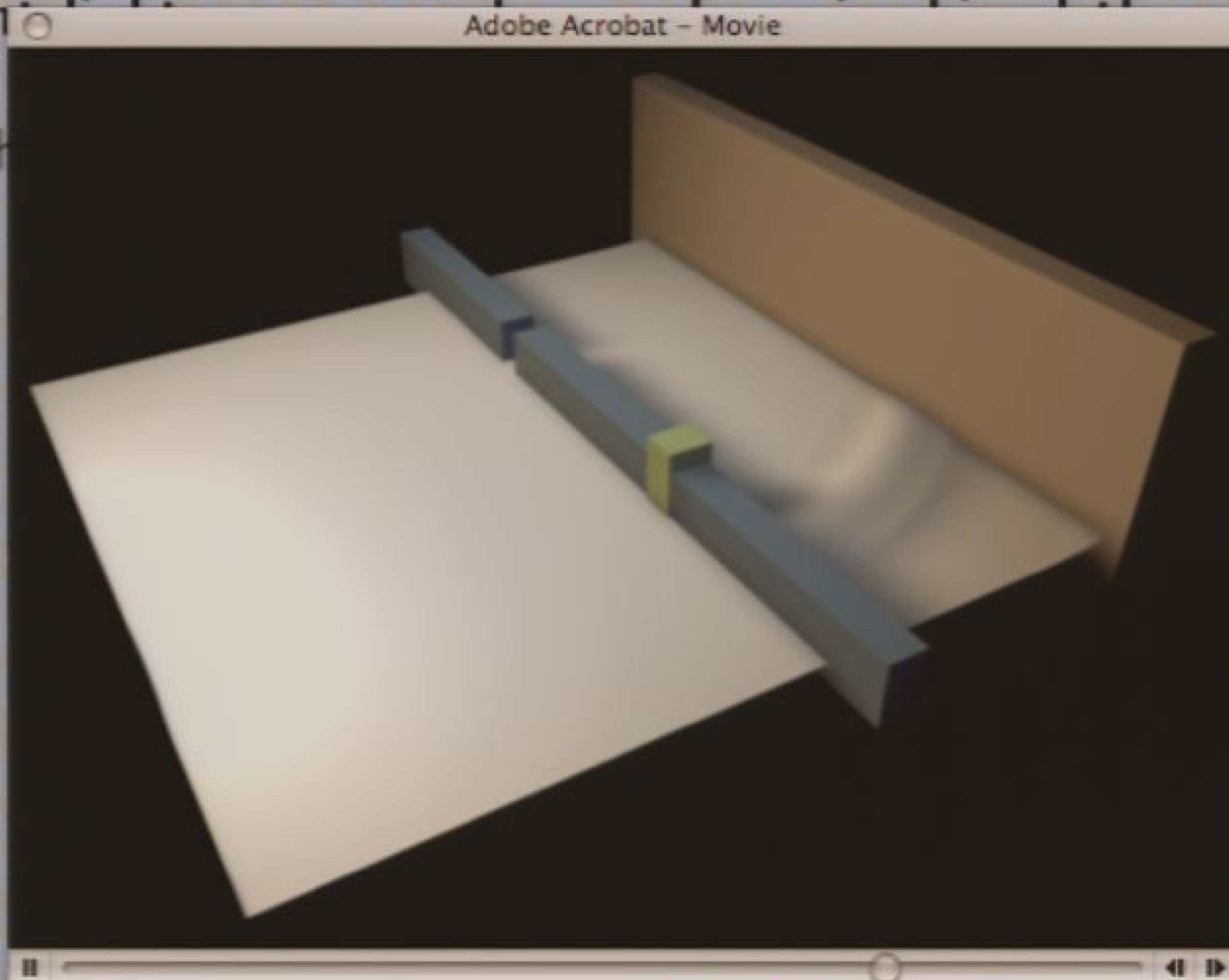
A coheren gh 2 slits,
the result final result
when both

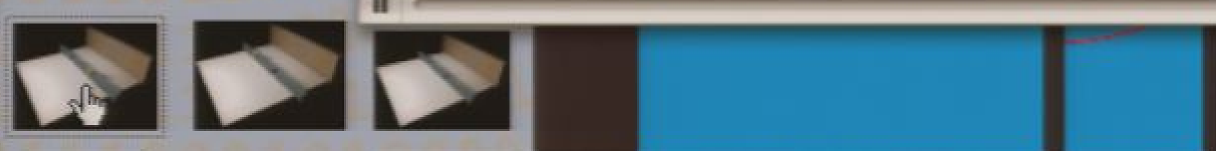




Basics of Quantum Mechanics

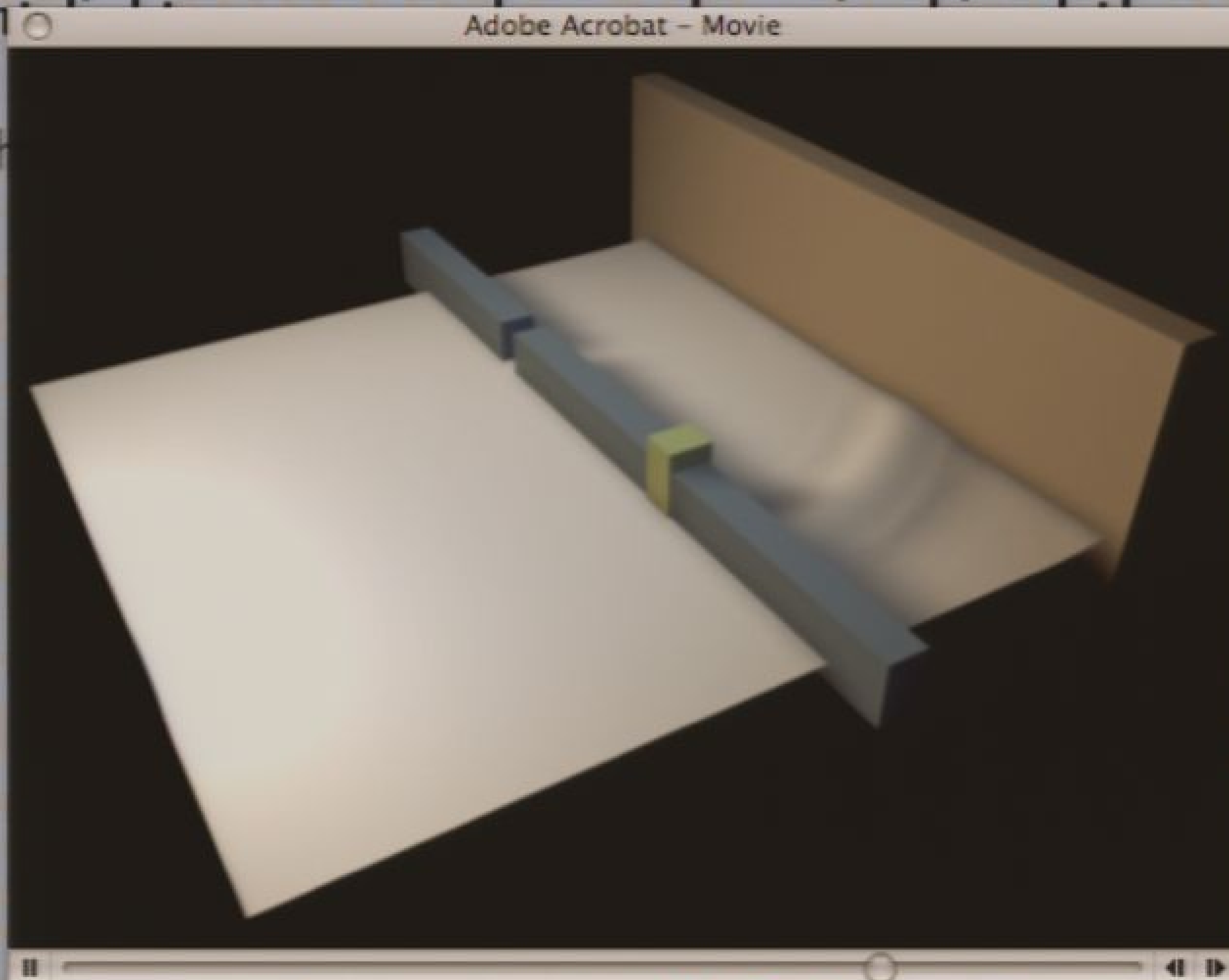
A coheren gh 2 slits,
the result final result
when both





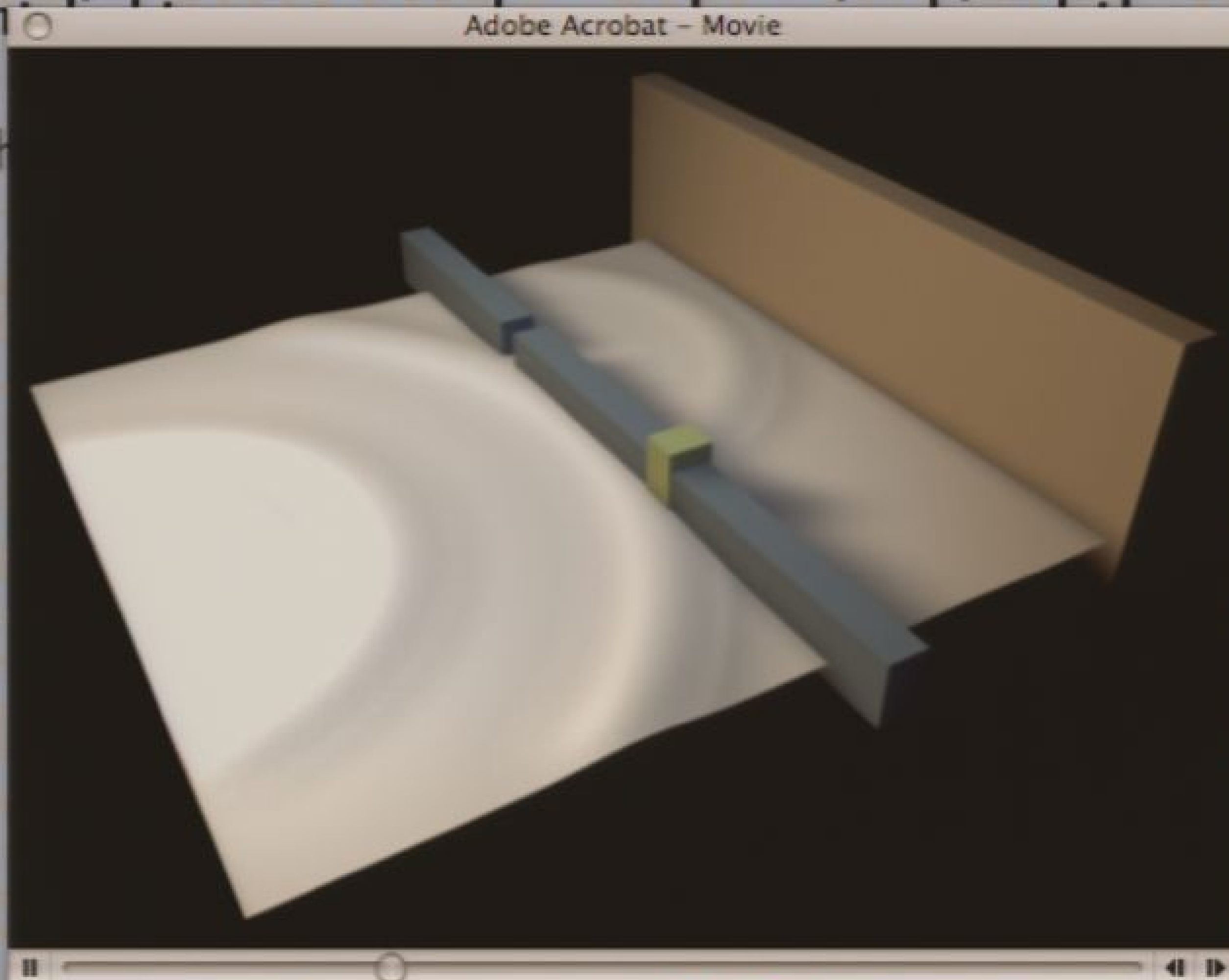
Basics of Quantum Mechanics

A coheren
gh 2 slits,
the result
final result
when both



Basics of Quantum Mechanics

A coheren **gh 2 slits,**
the result **final result**
when both

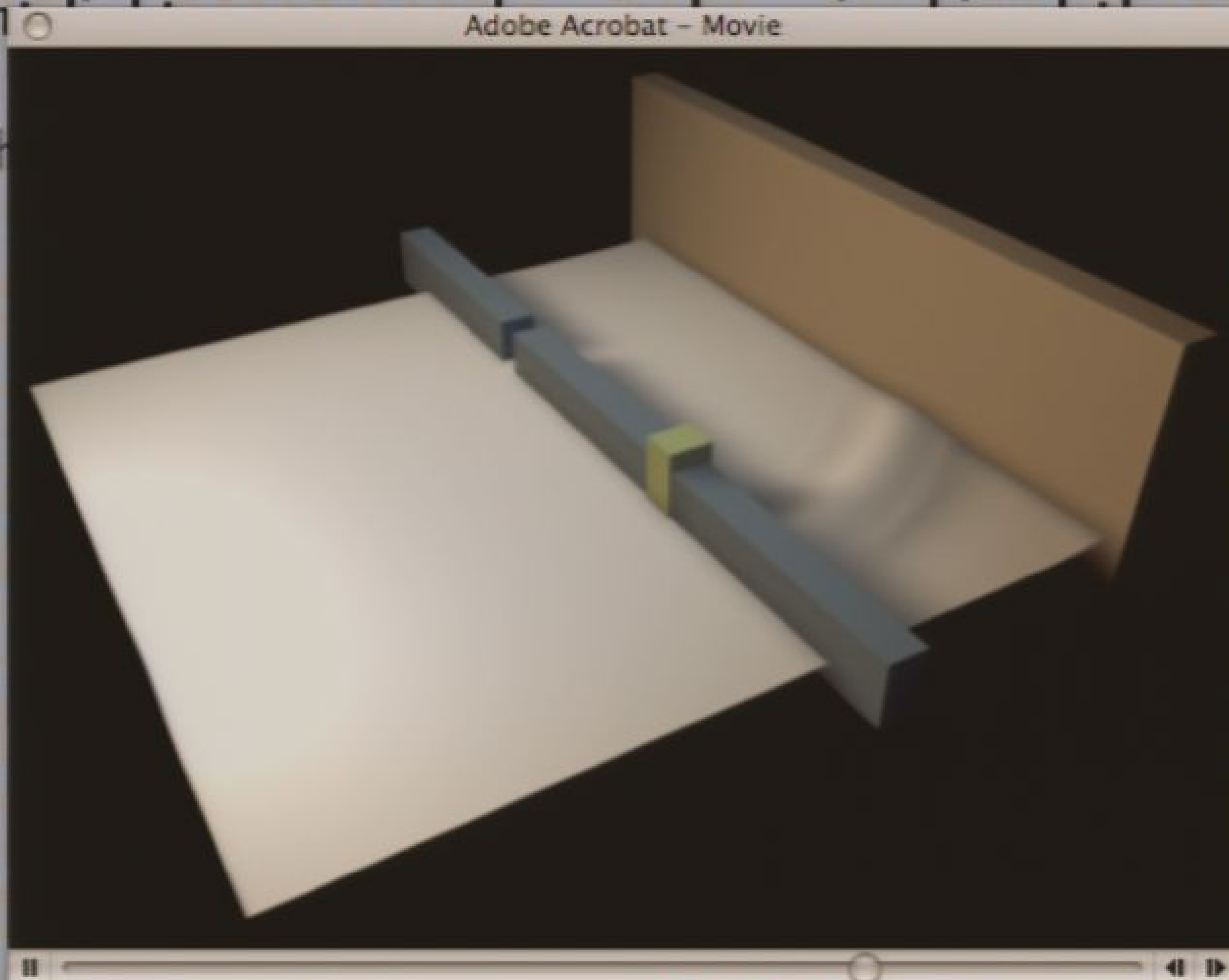


Basics of Quantum Mechanics

A coheren

the result

when both

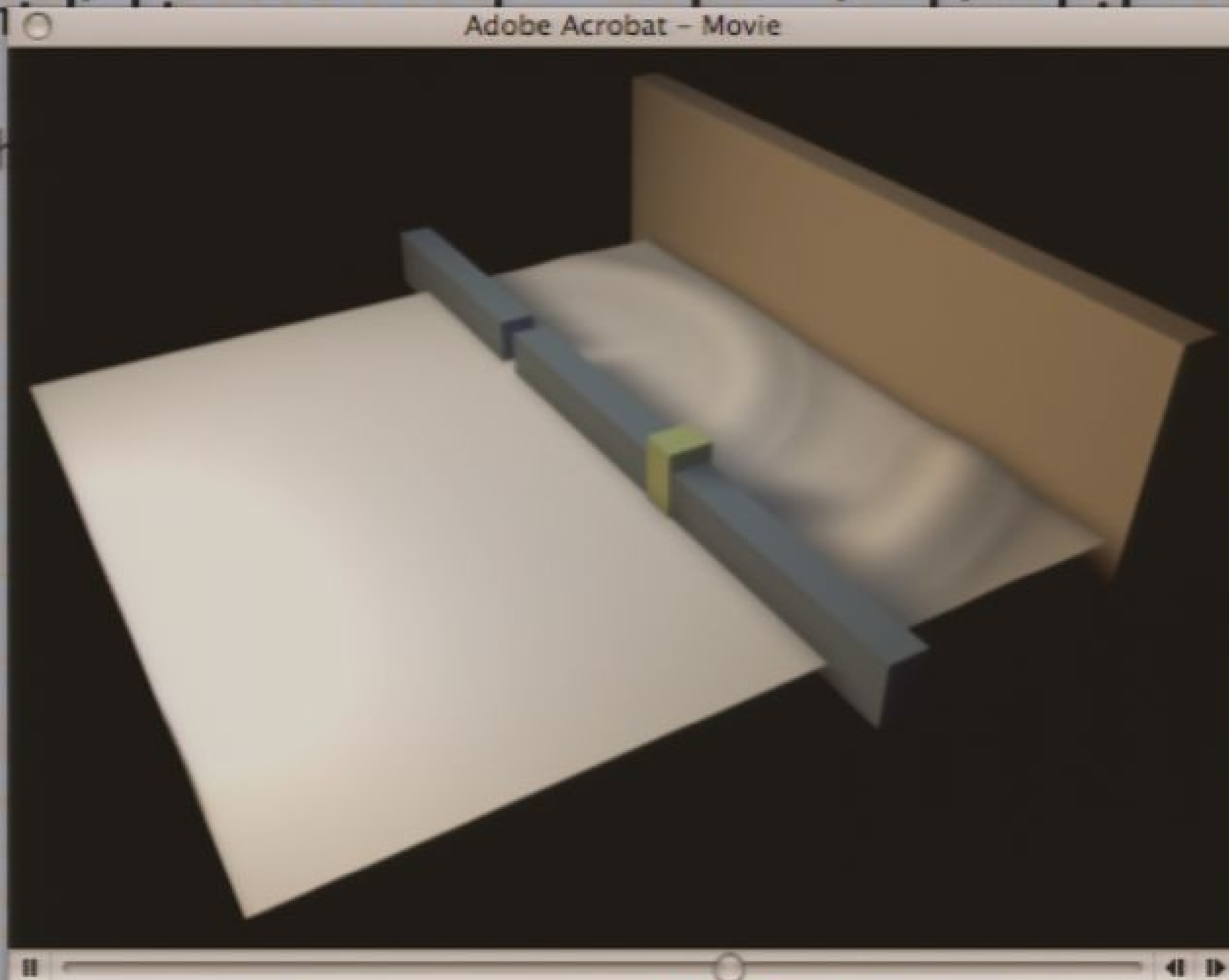


gh 2 slits,

final result

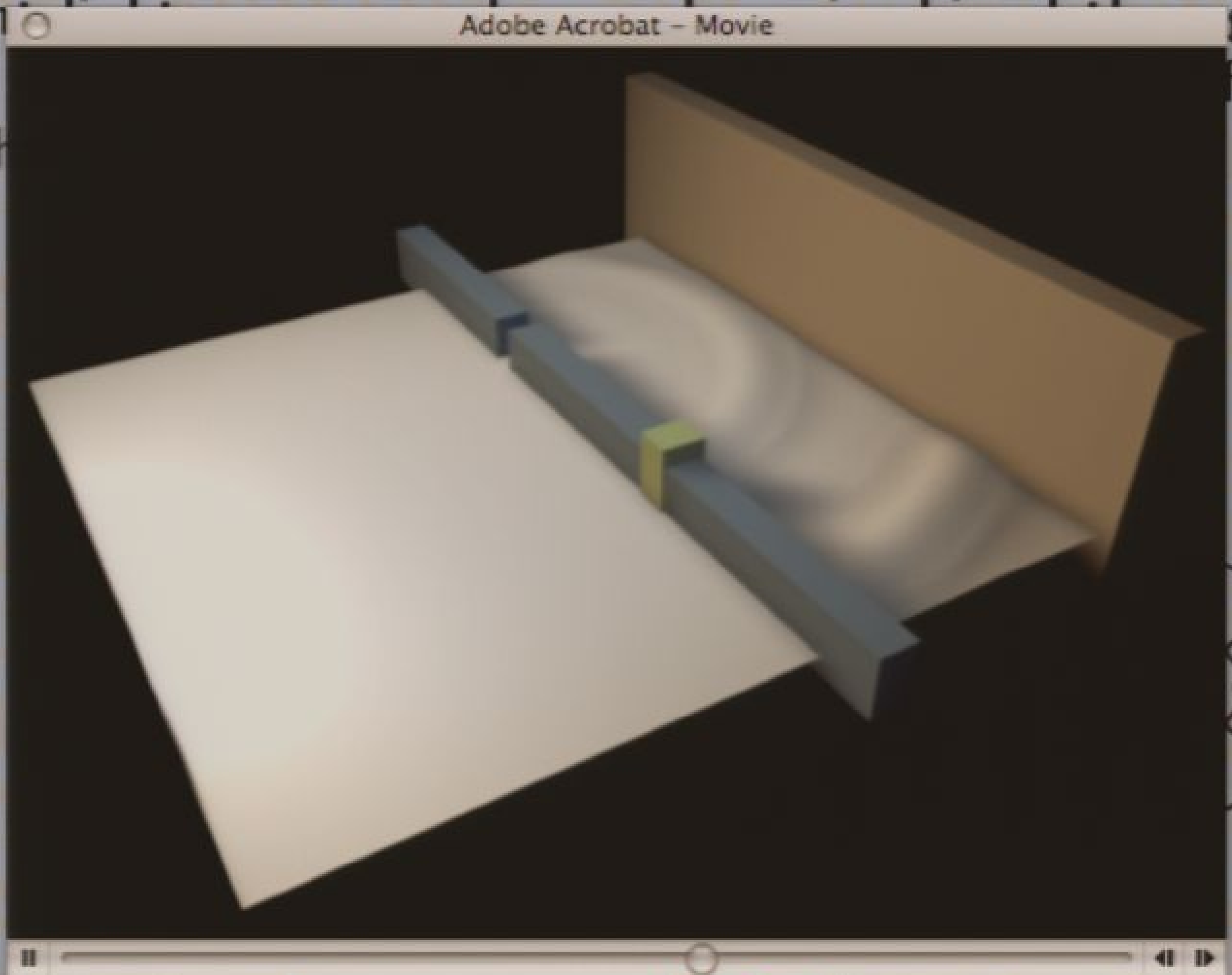
Basics of Quantum Mechanics

A coheren ... gh 2 slits,
the result ... final result
when both



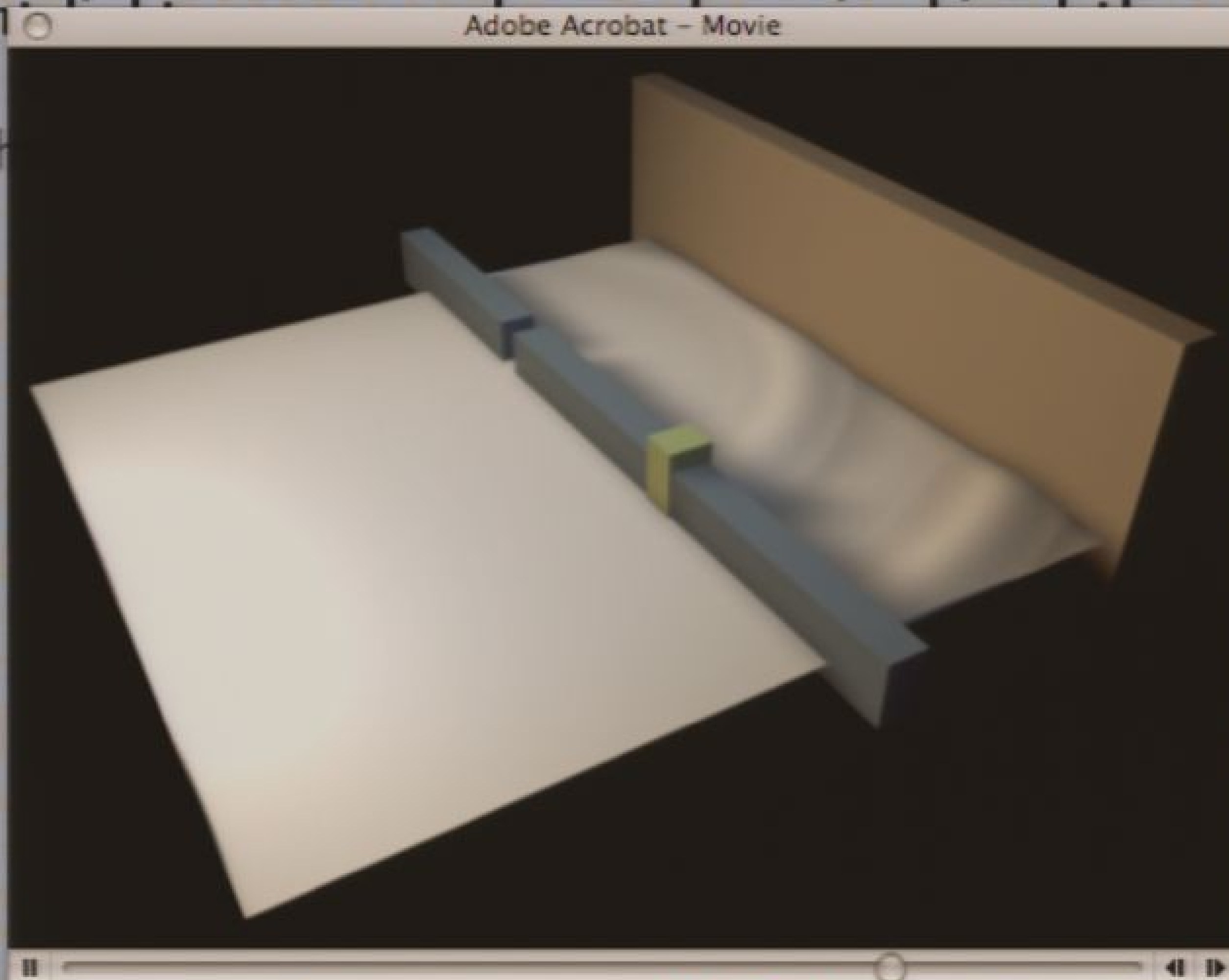
Basics of Quantum Mechanics

A coheren[…]**gh 2 slits, the result**[…]**final result when both**[…]



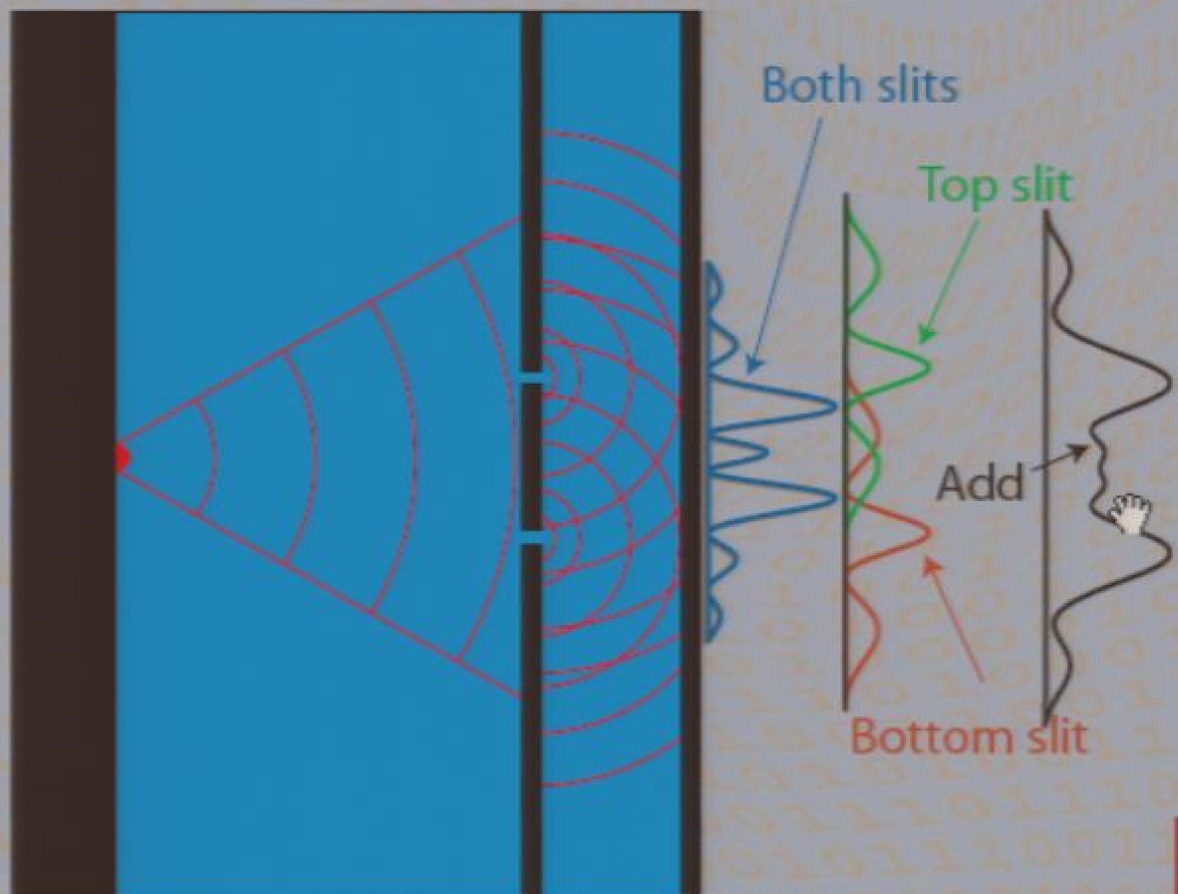
Basics of Quantum Mechanics

A coheren **gh 2 slits,**
the result **final result**
when both



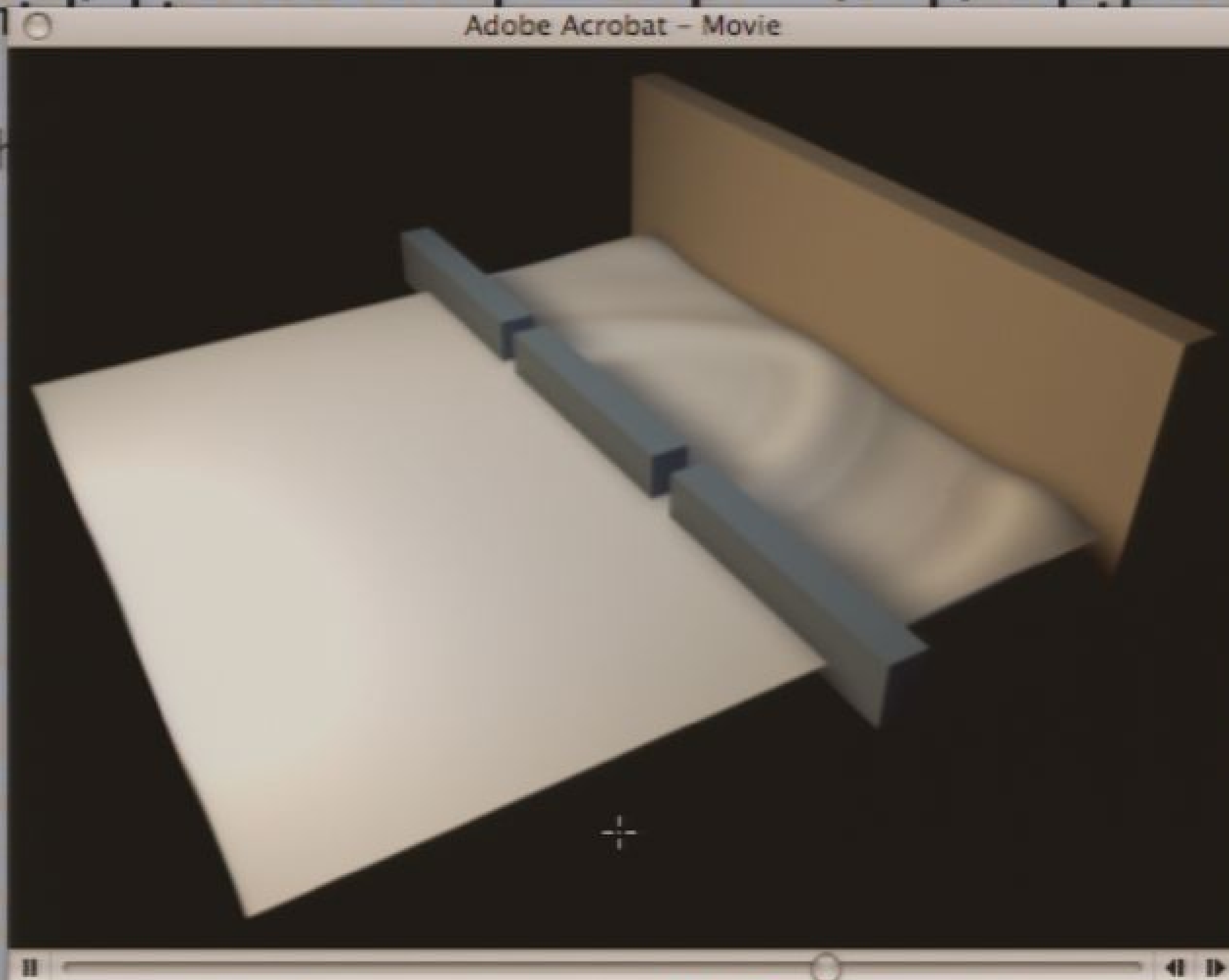
Basics of Quantum Mechanics

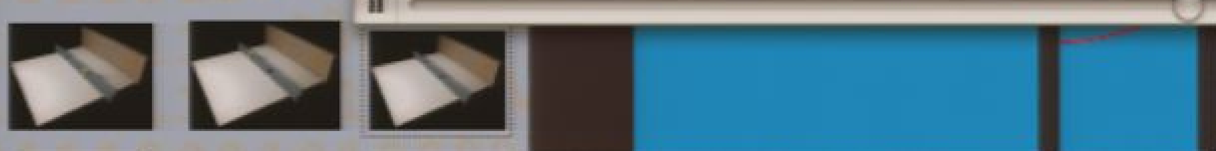
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

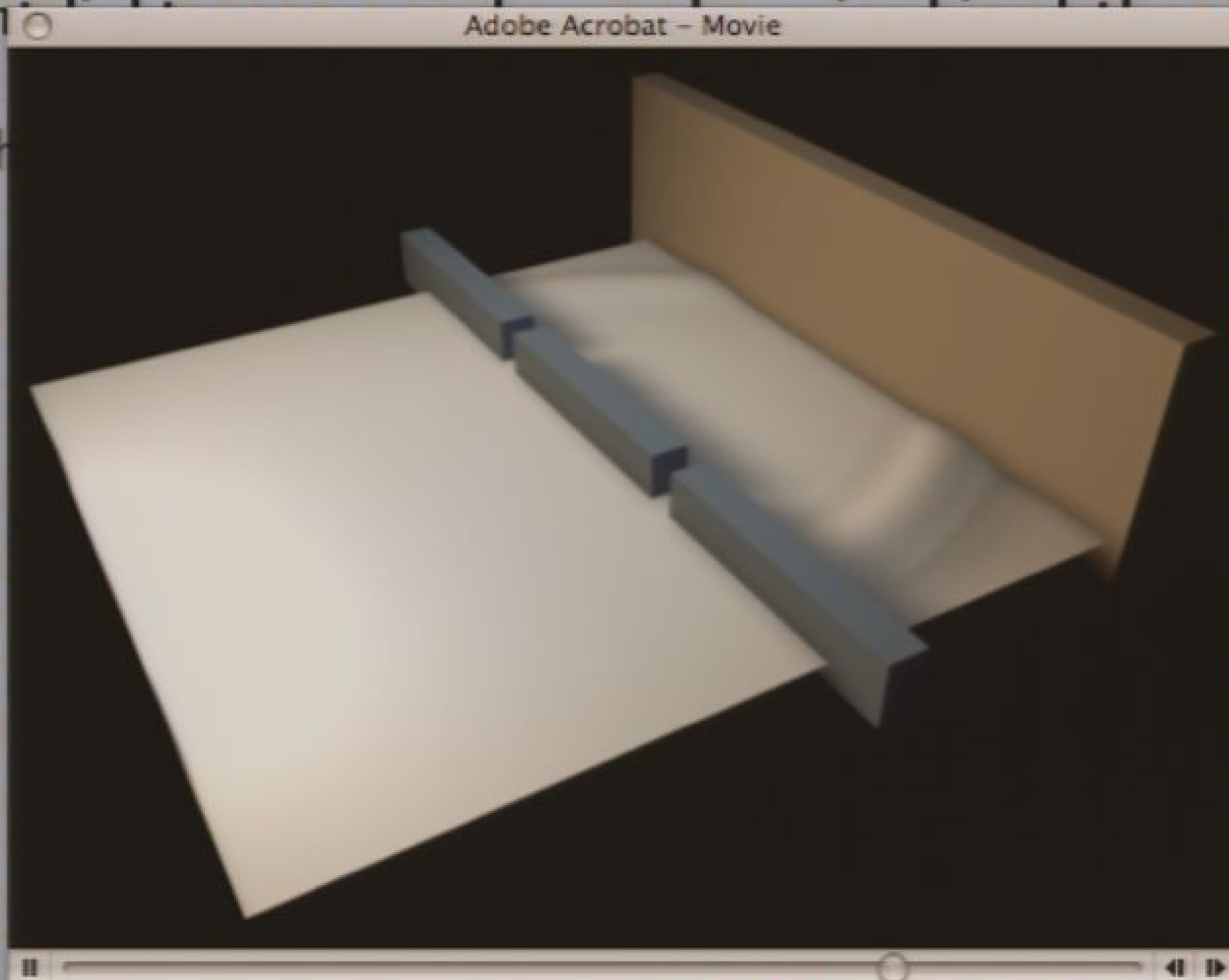
A coheren… gh 2 slits, the result … final result when both…





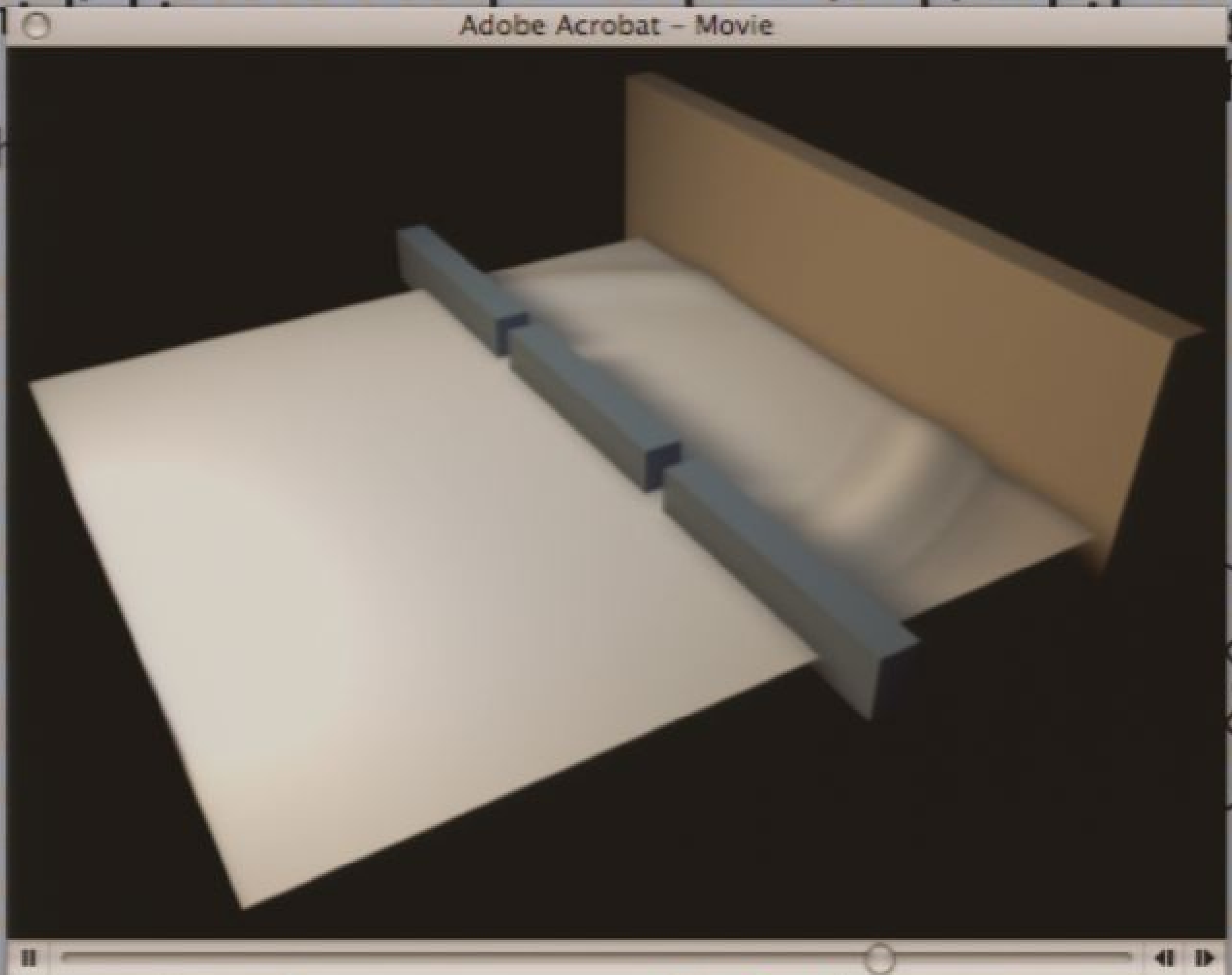
Basics of Quantum Mechanics

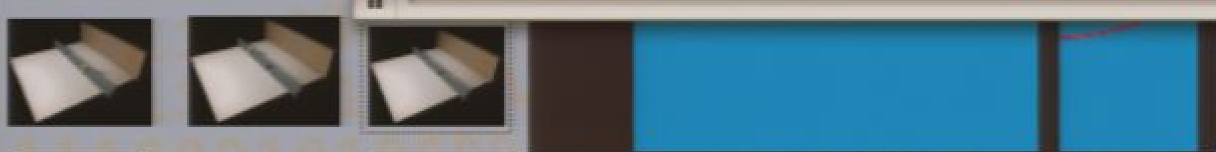
A coheren[...]gh 2 slits, the result [...] final result when both[...]



Basics of Quantum Mechanics

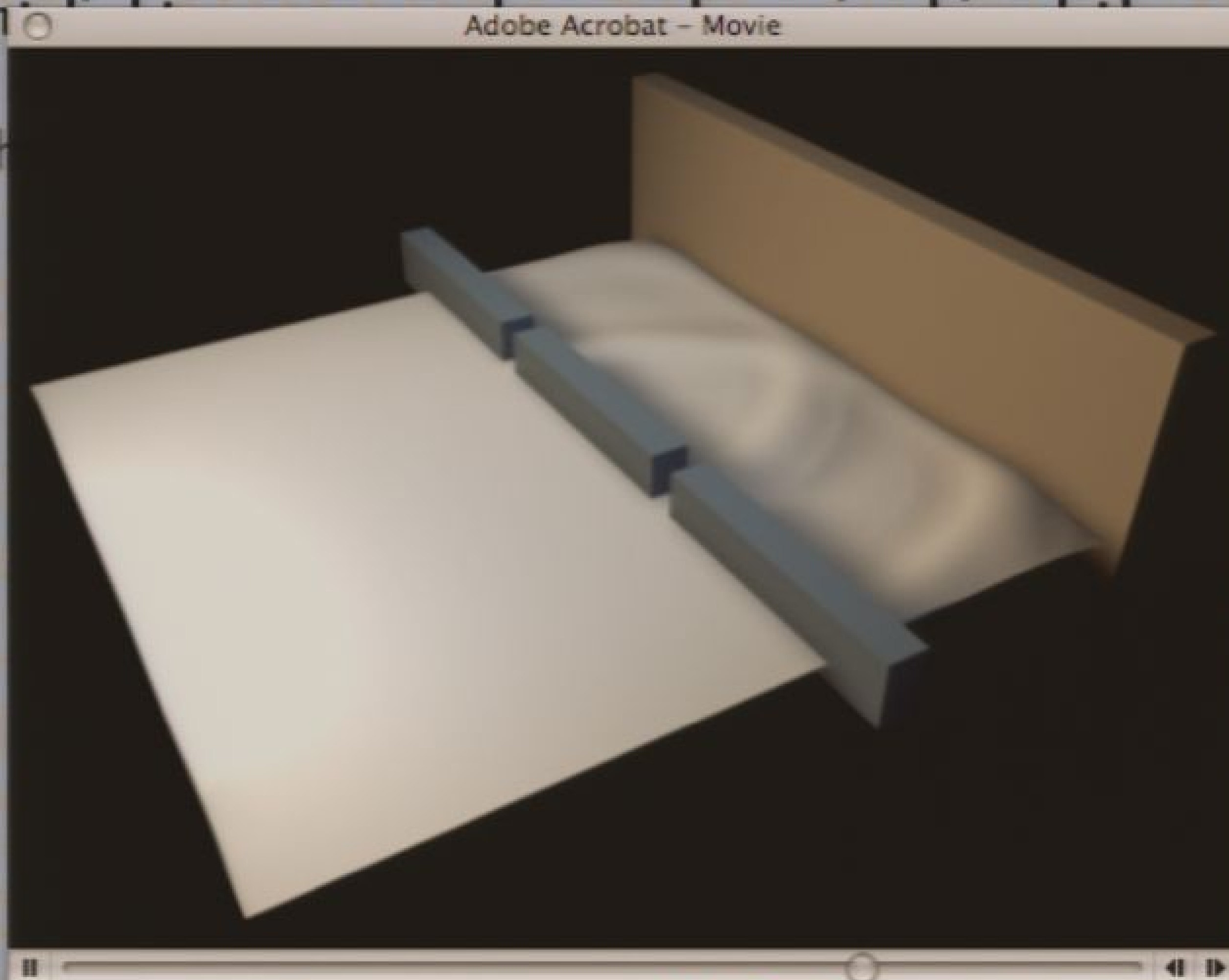
A coheren[...] **gh 2 slits,**
the result [...] **final result**
when both

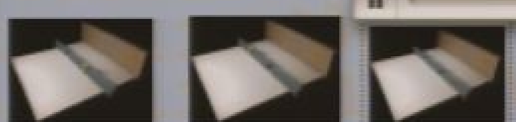




Basics of Quantum Mechanics

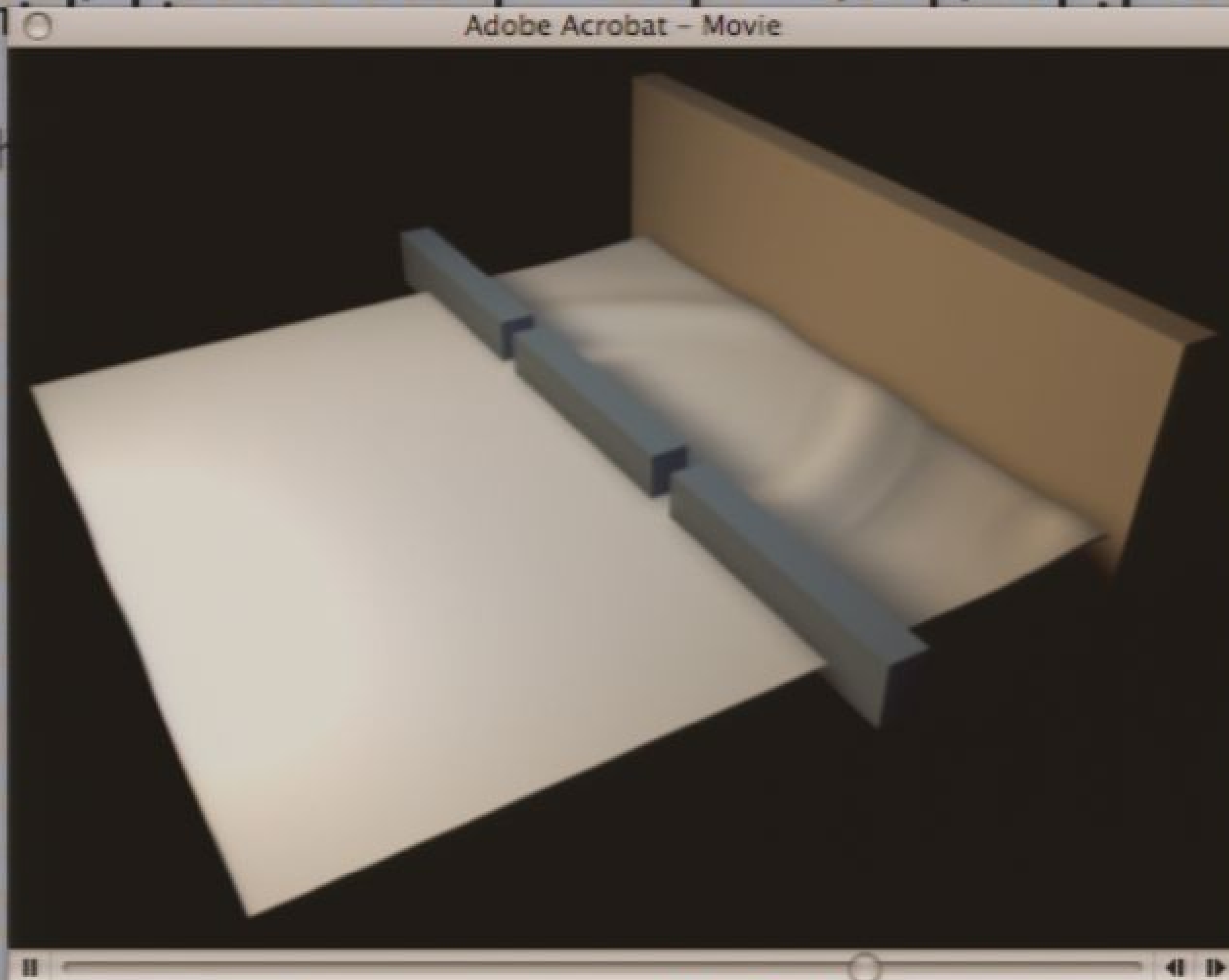
A coheren … **gh 2 slits,**
the result … **final result**
when both …

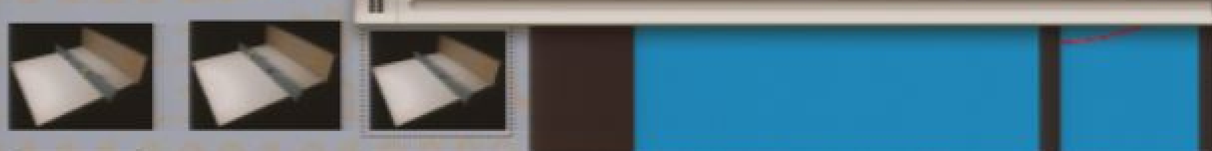




Basics of Quantum Mechanics

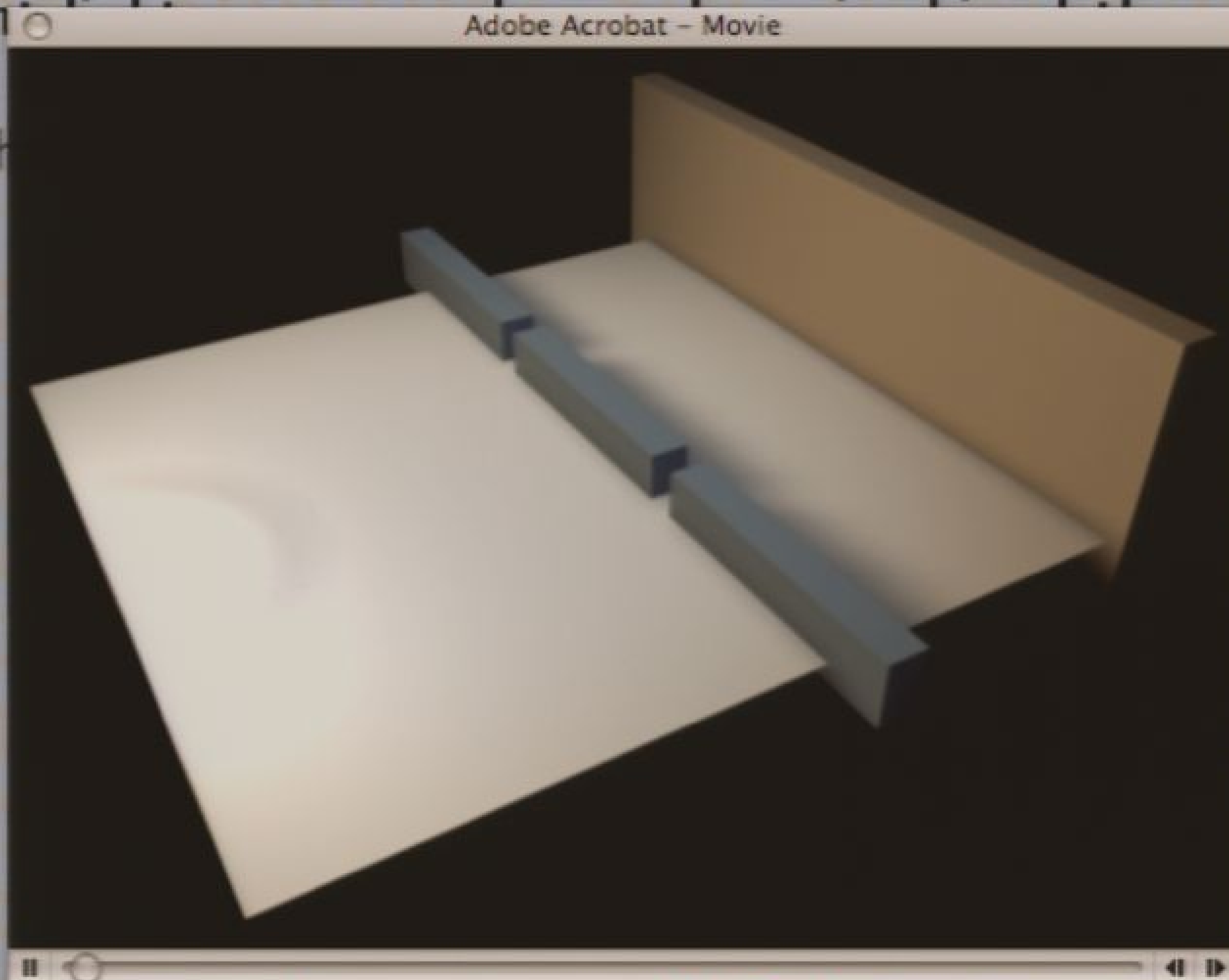
A coheren … **gh 2 slits,**
the result … **final result**
when both

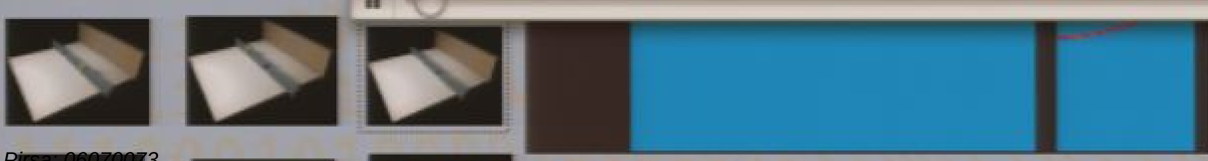




Basics of Quantum Mechanics

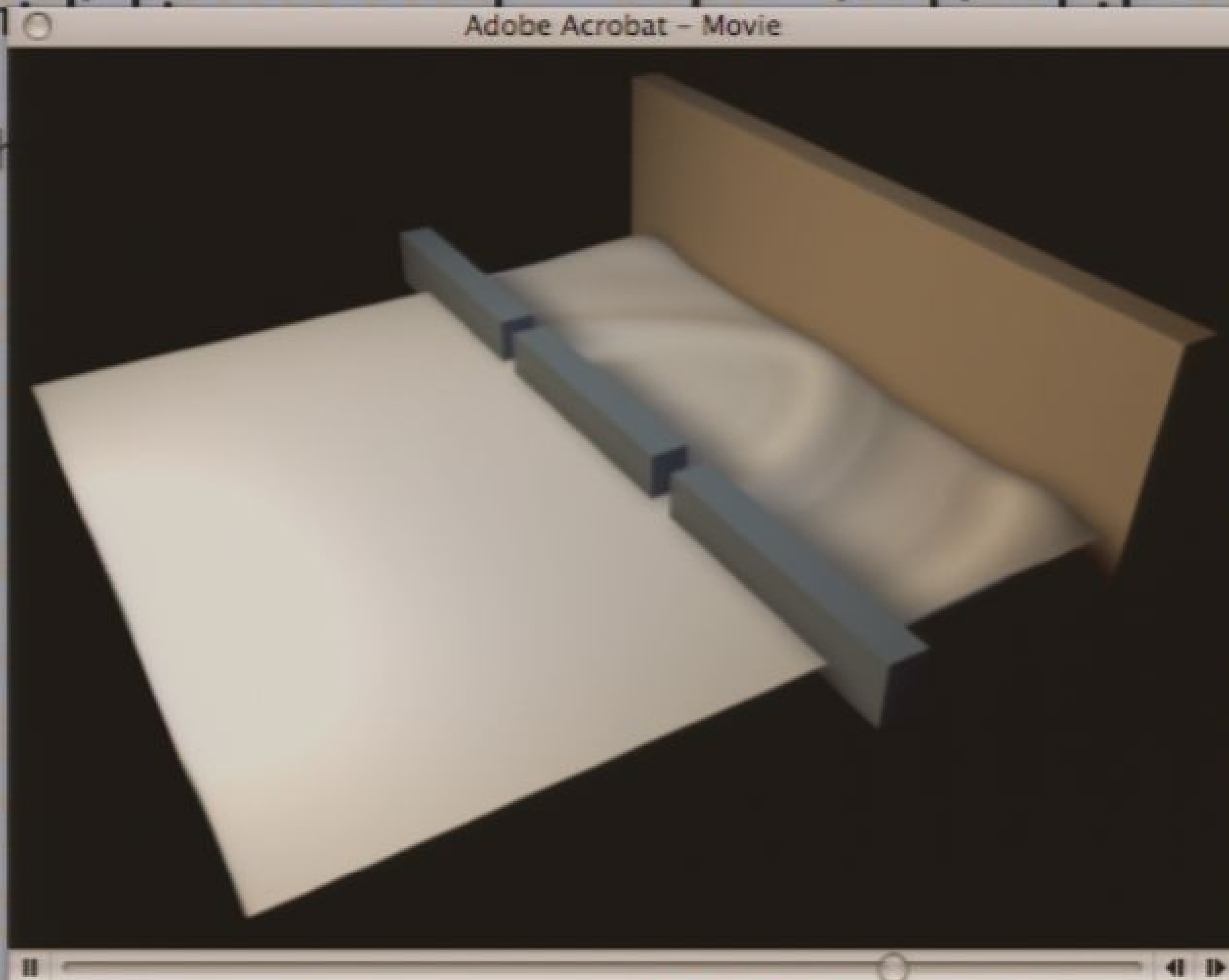
A coheren... gh 2 slits,
the result ... final result
when both

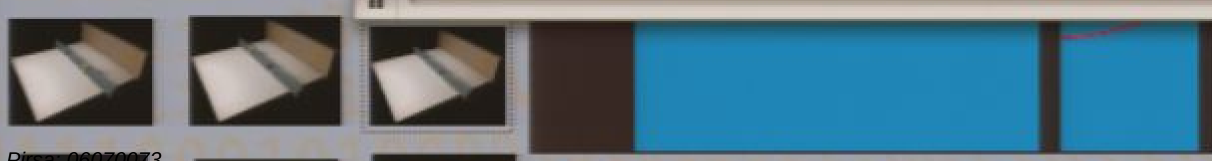




Basics of Quantum Mechanics

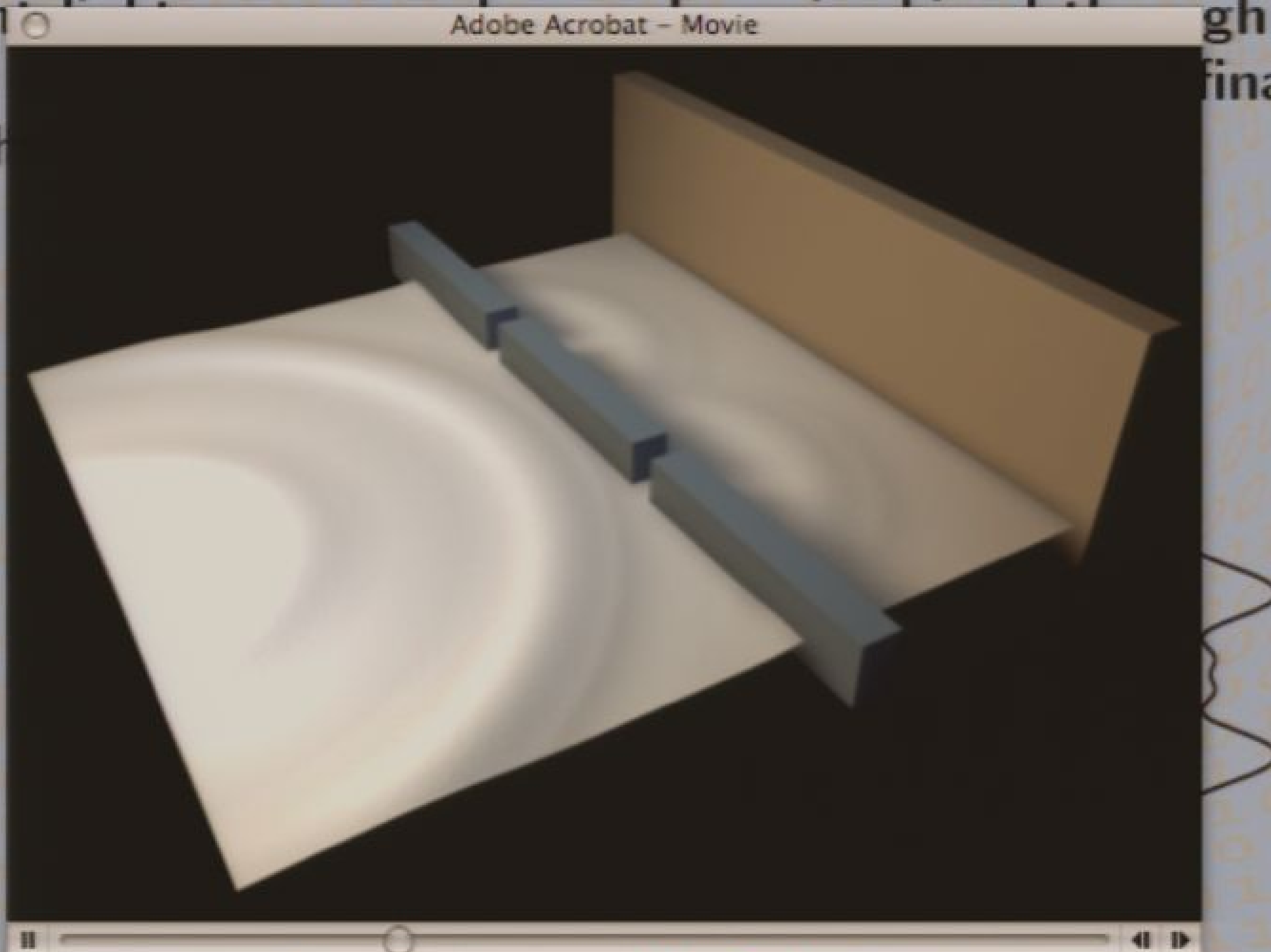
A coheren … **gh 2 slits,**
the result … **final result**
when both





Basics of Quantum Mechanics

A coheren gh 2 slits,
the result final result
when both



Basics of Quantum Mechanics

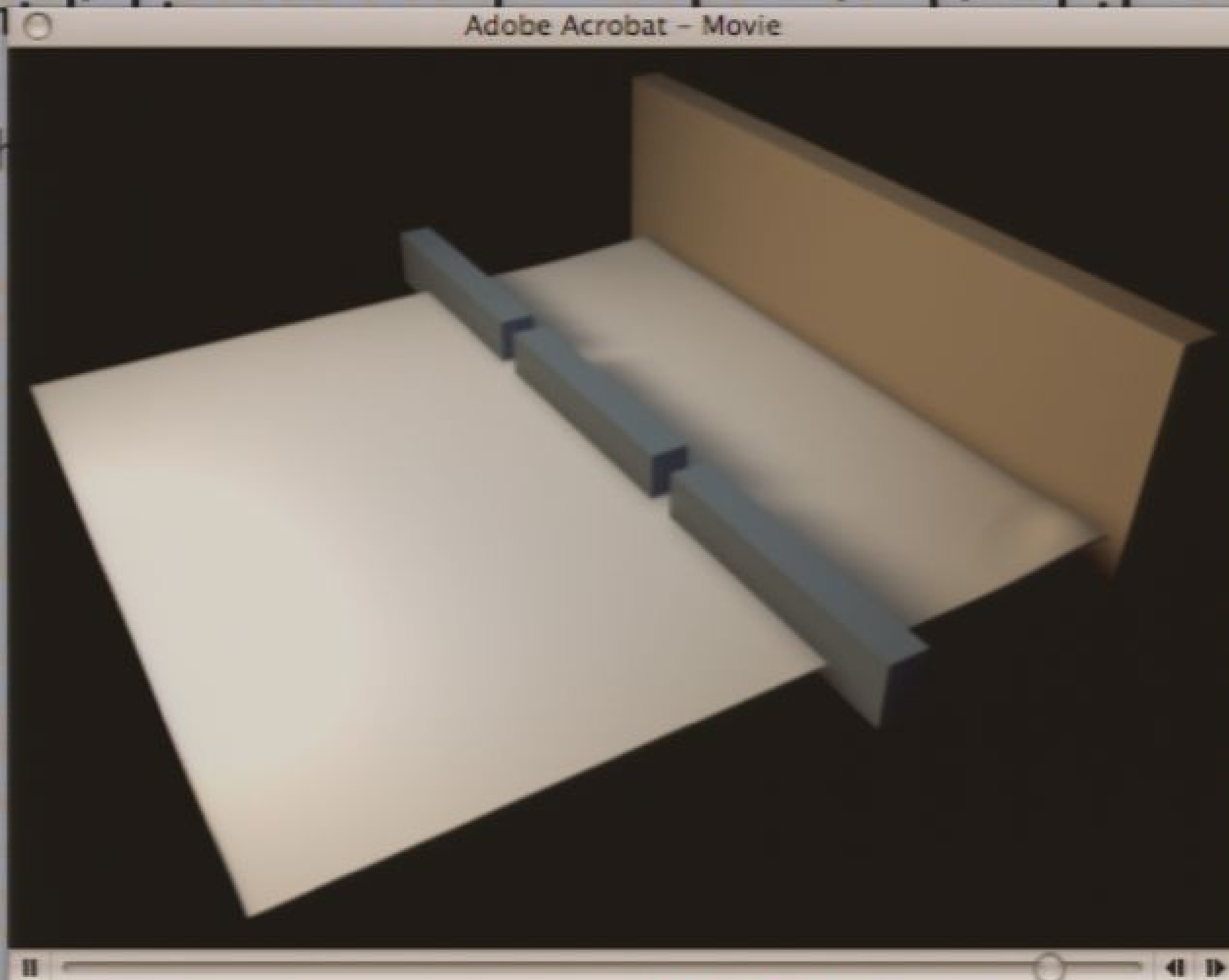
A coheren

gh 2 slits,

the result

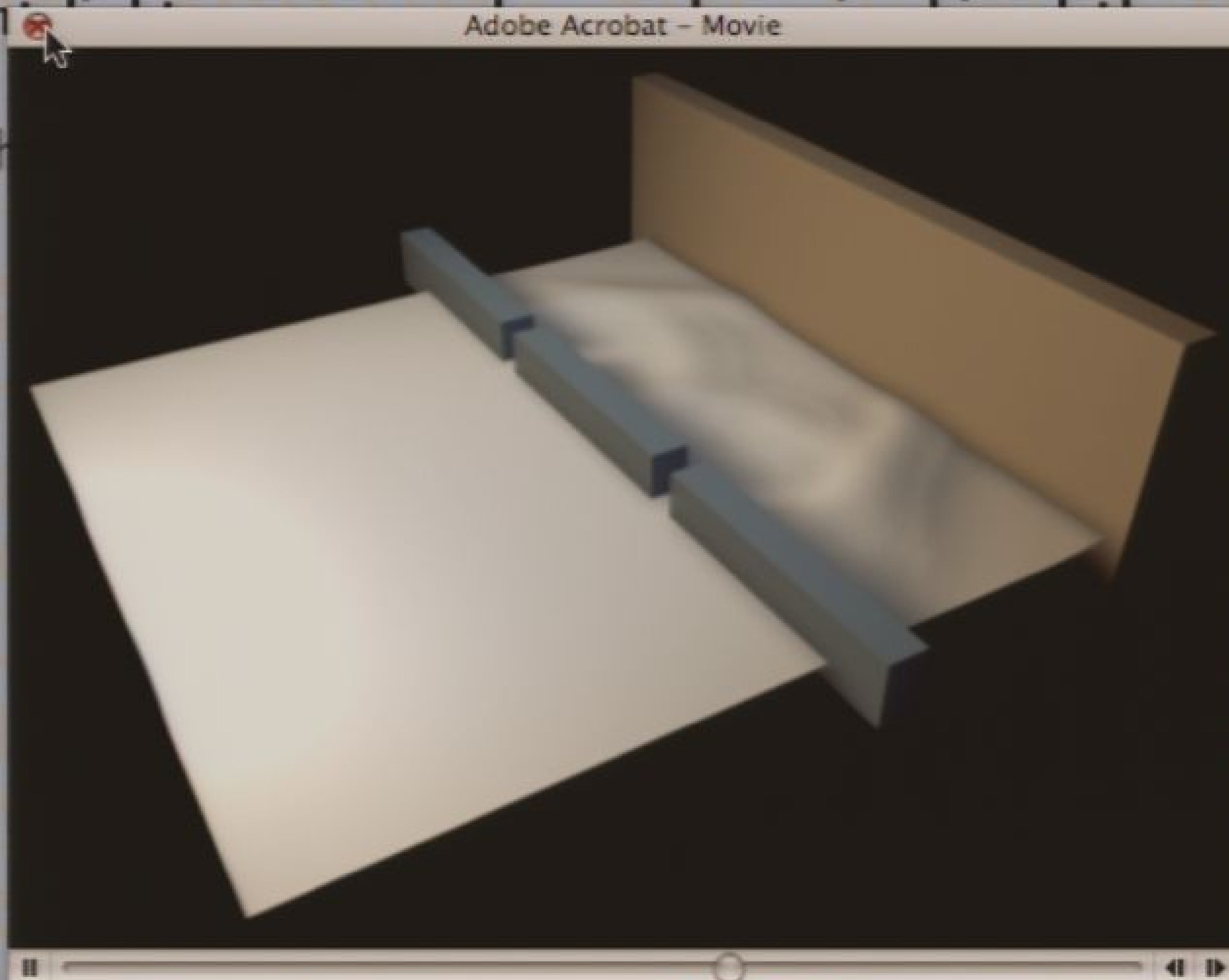
final result

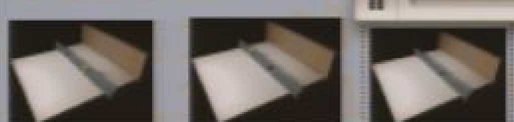
when both



Basics of Quantum Mechanics

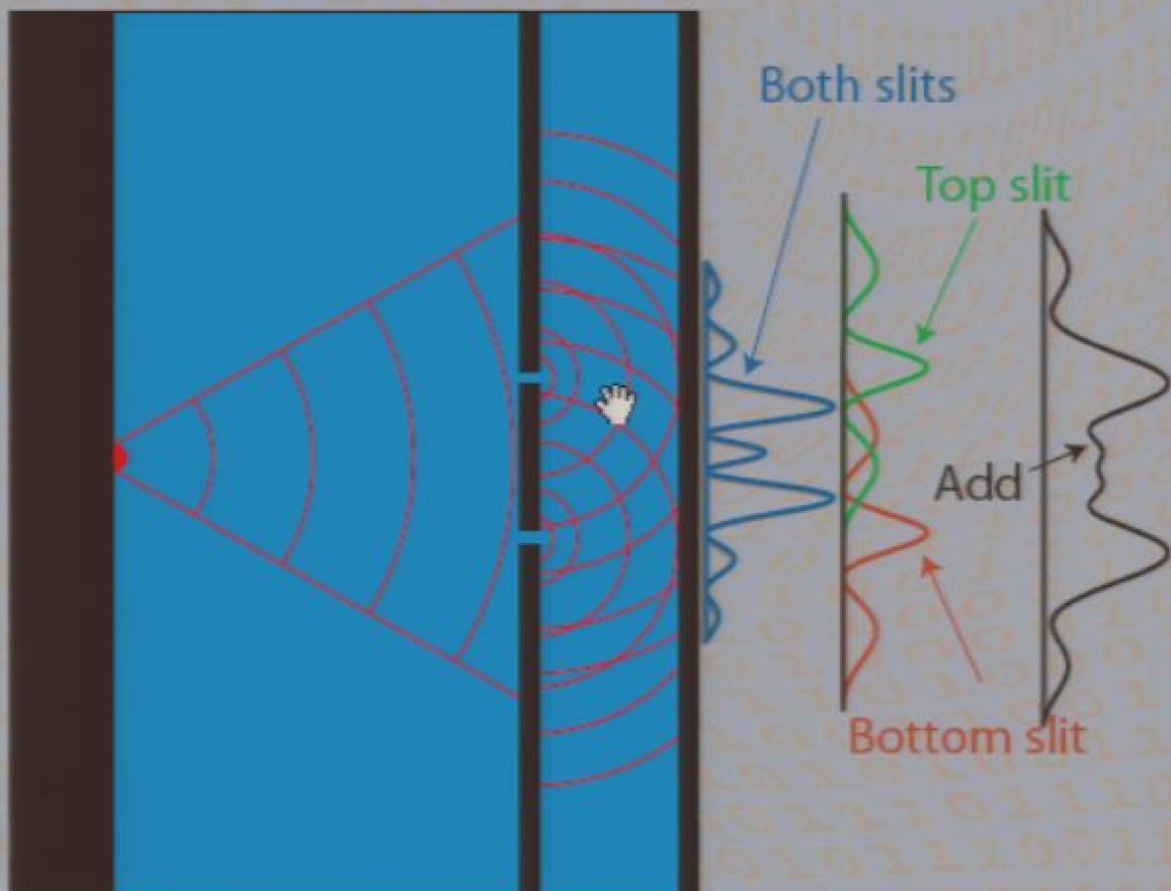
A coheren… …gh 2 slits,
the result … …final result
when both…





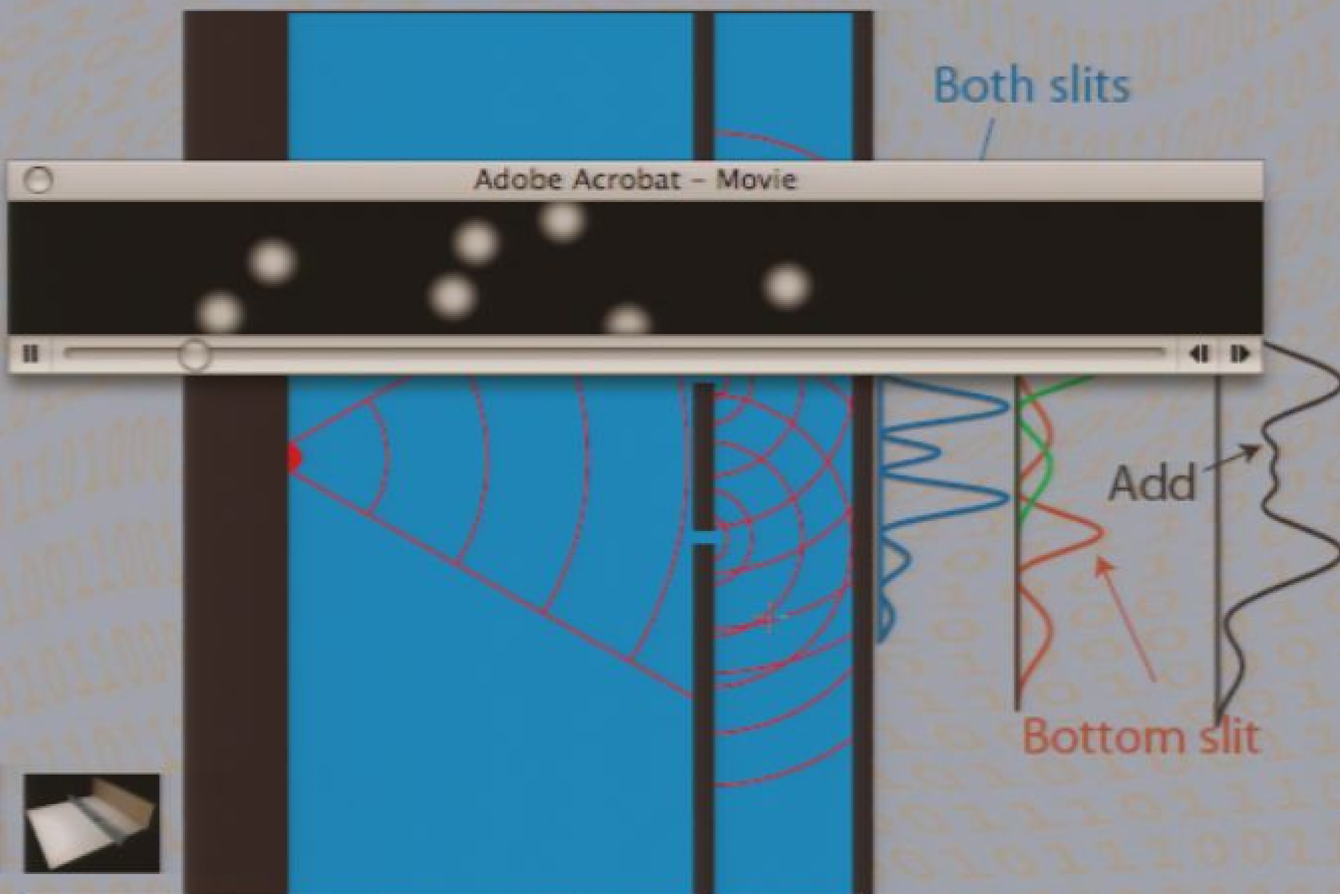
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



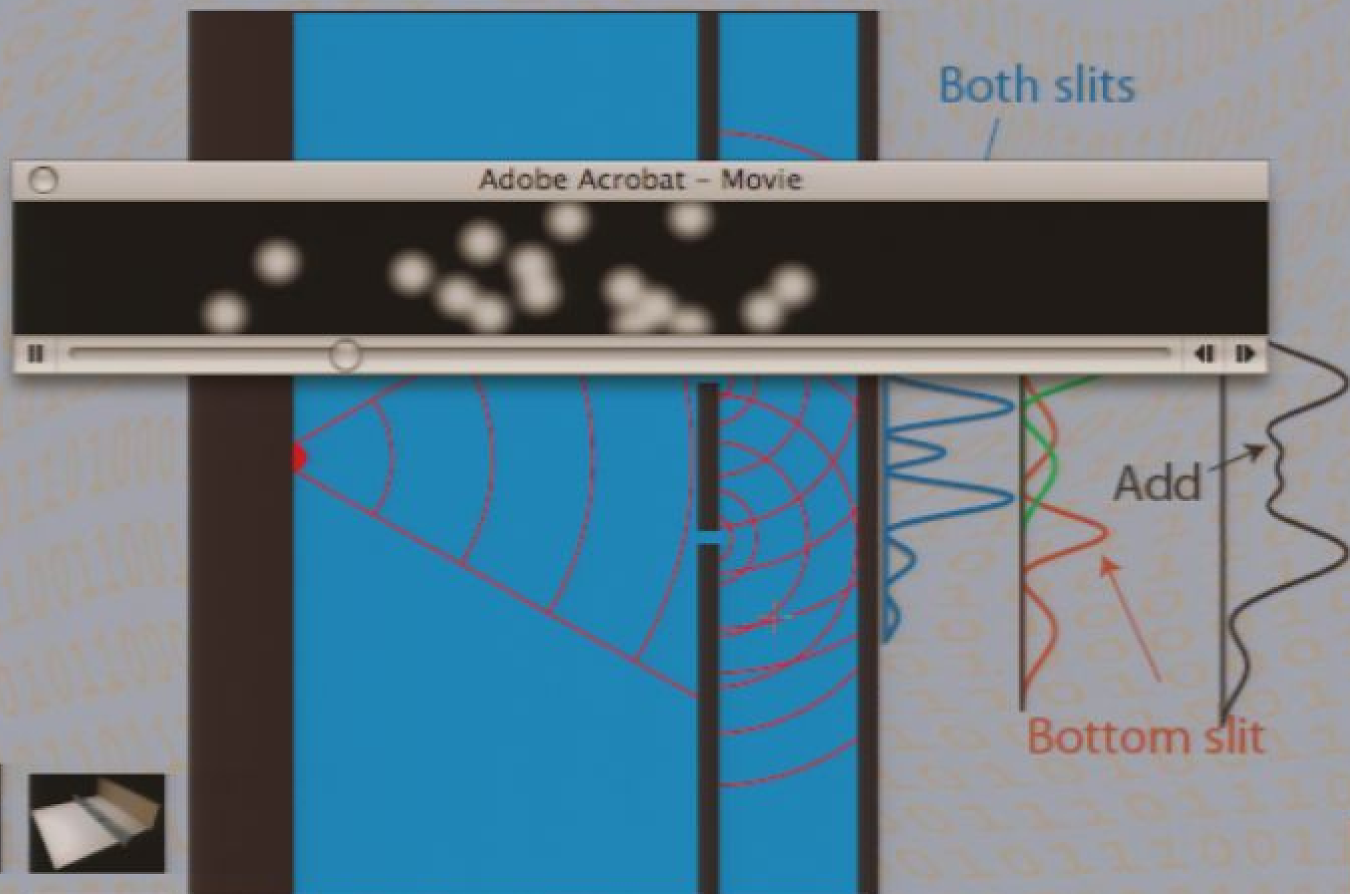
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



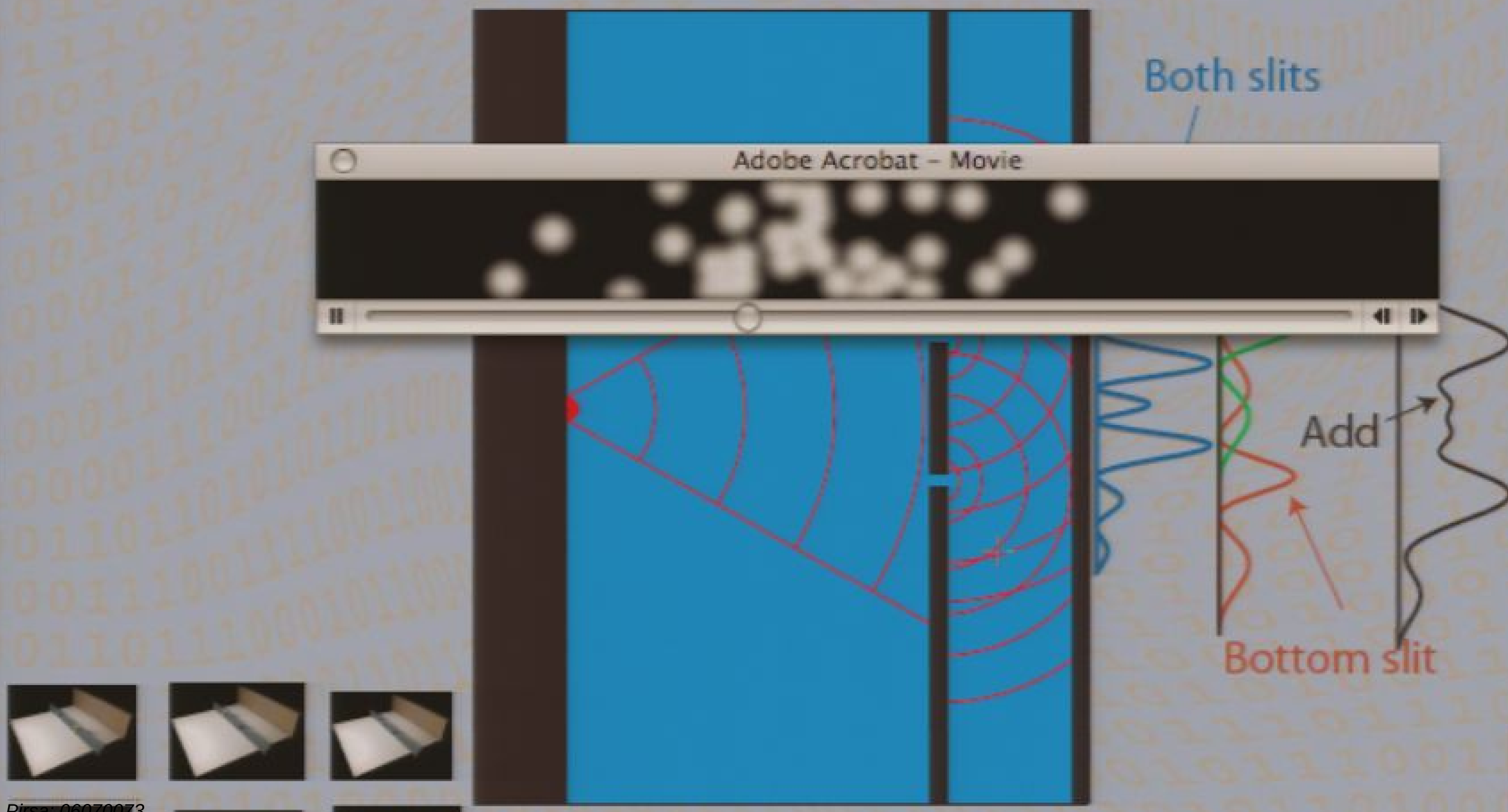
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



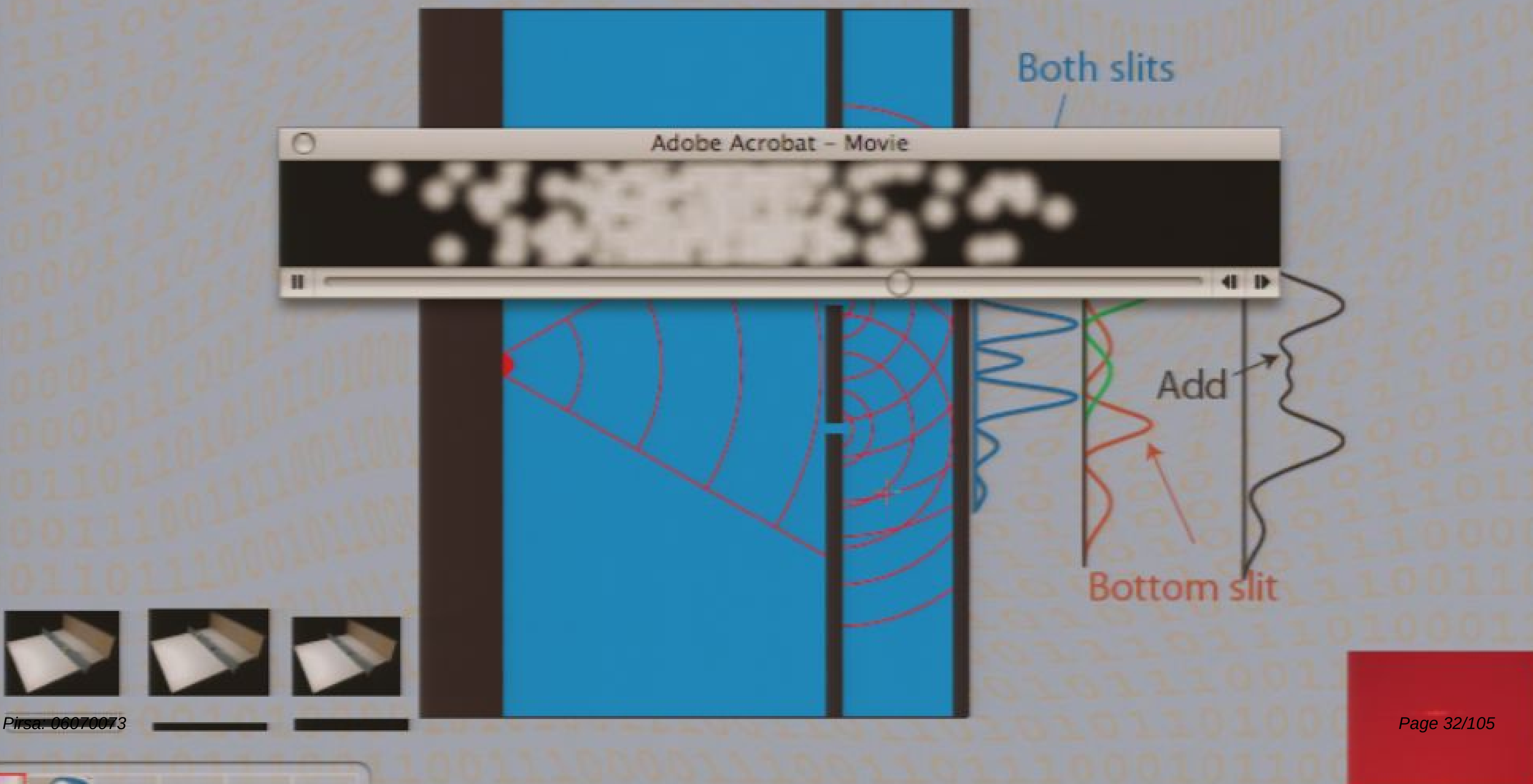
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



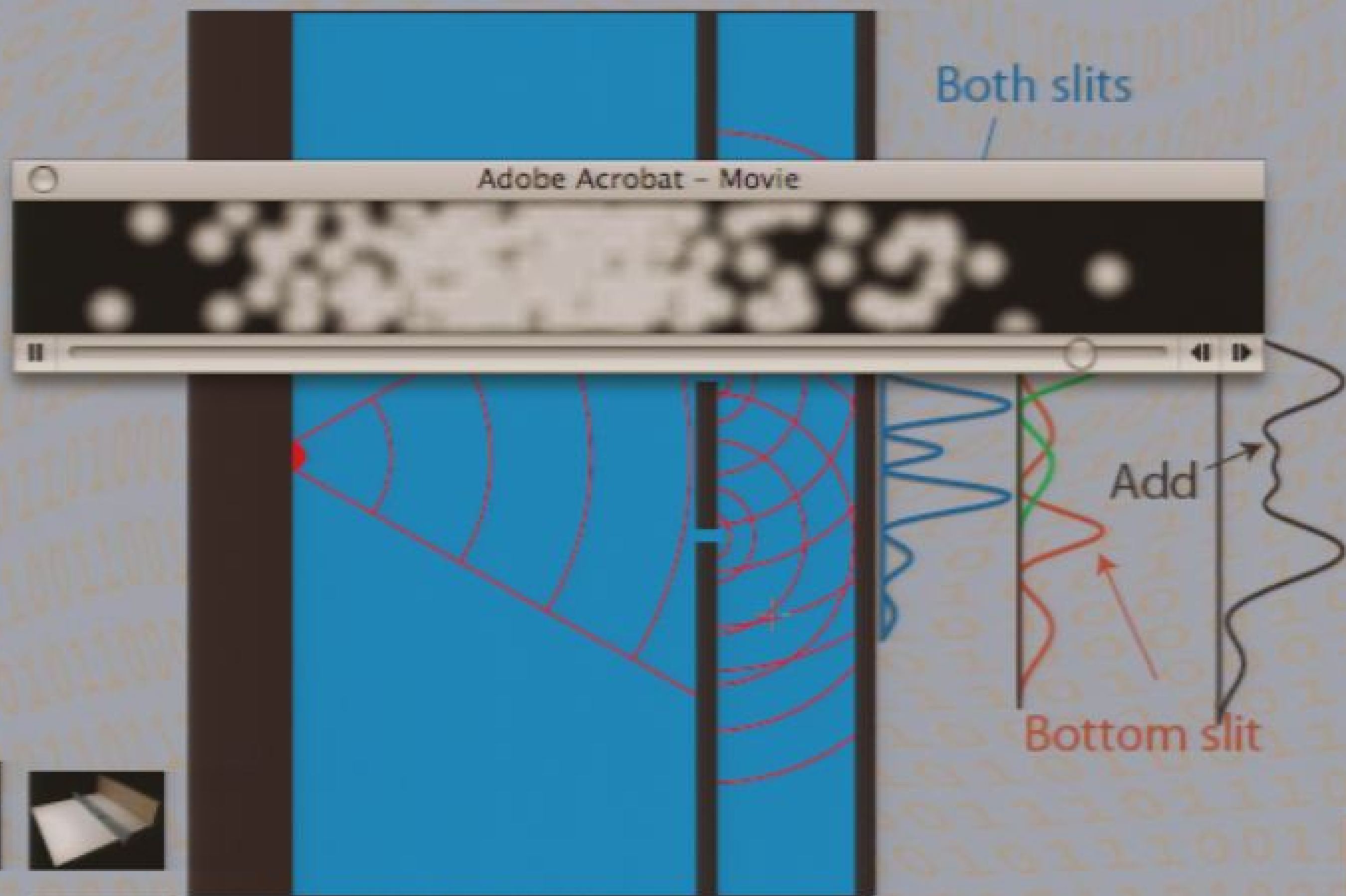
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



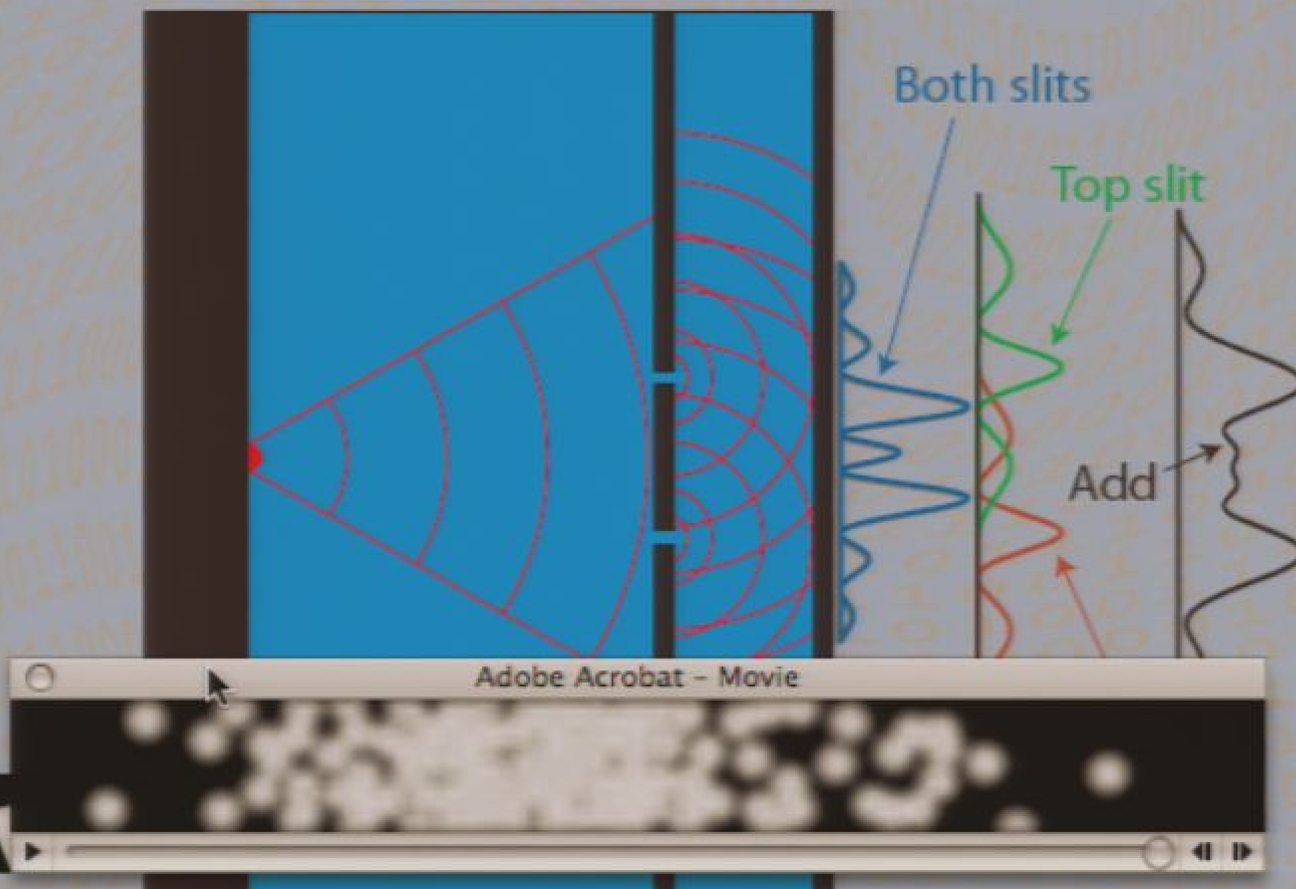
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



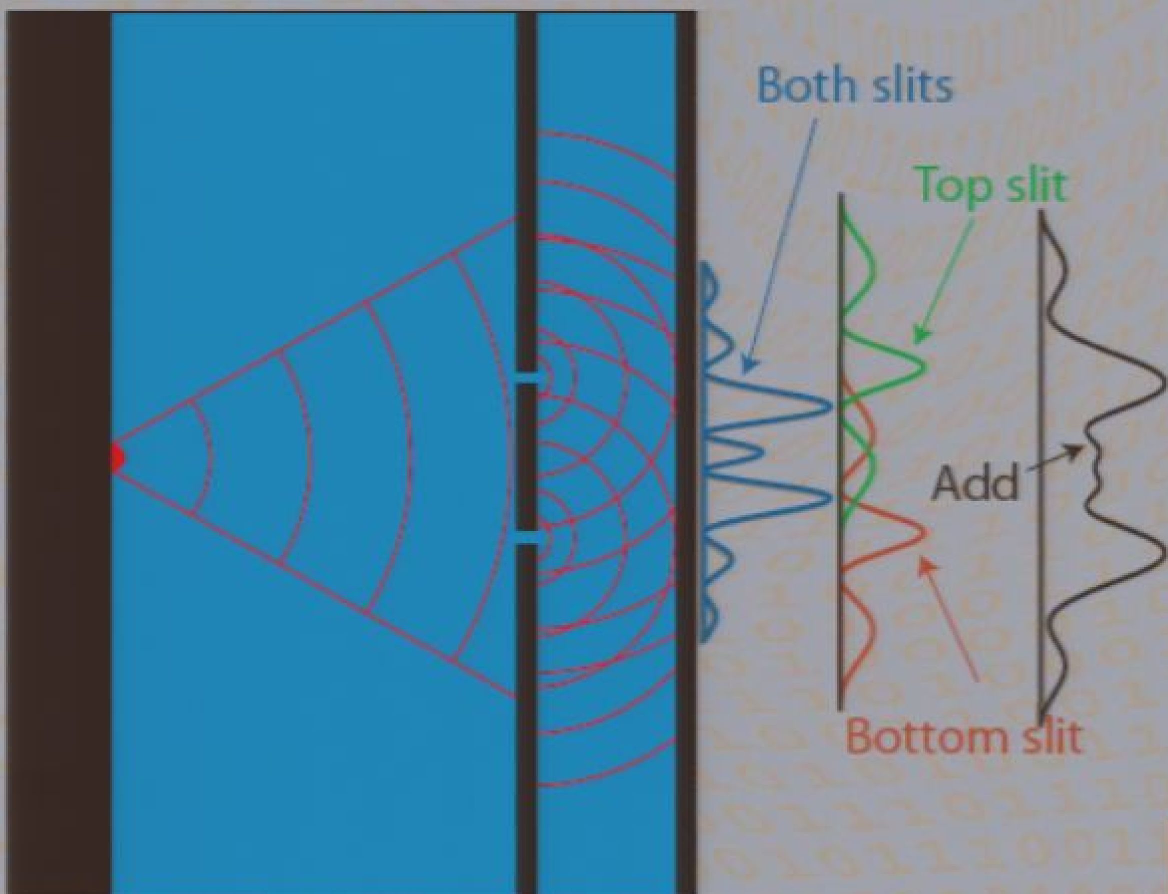
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



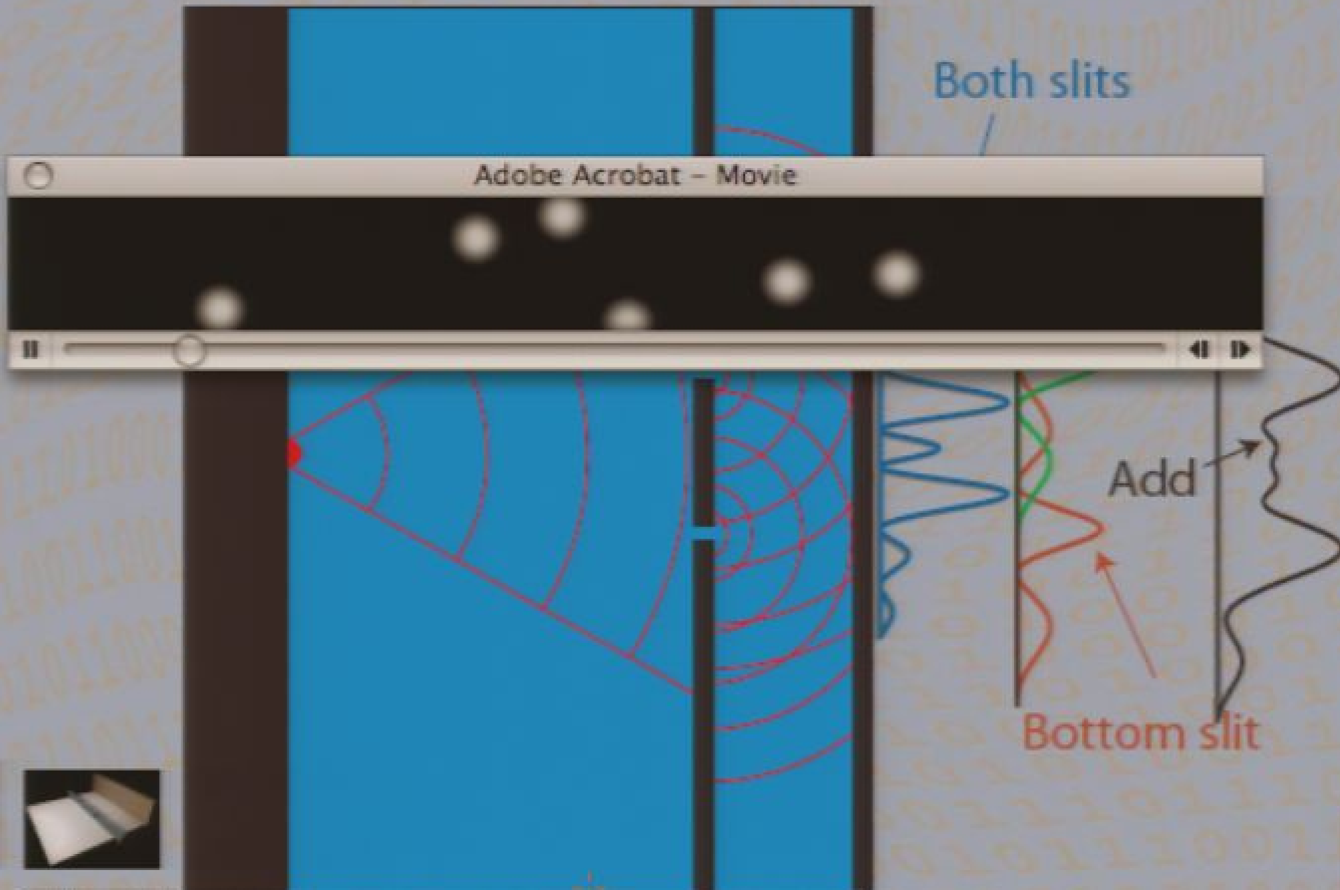
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



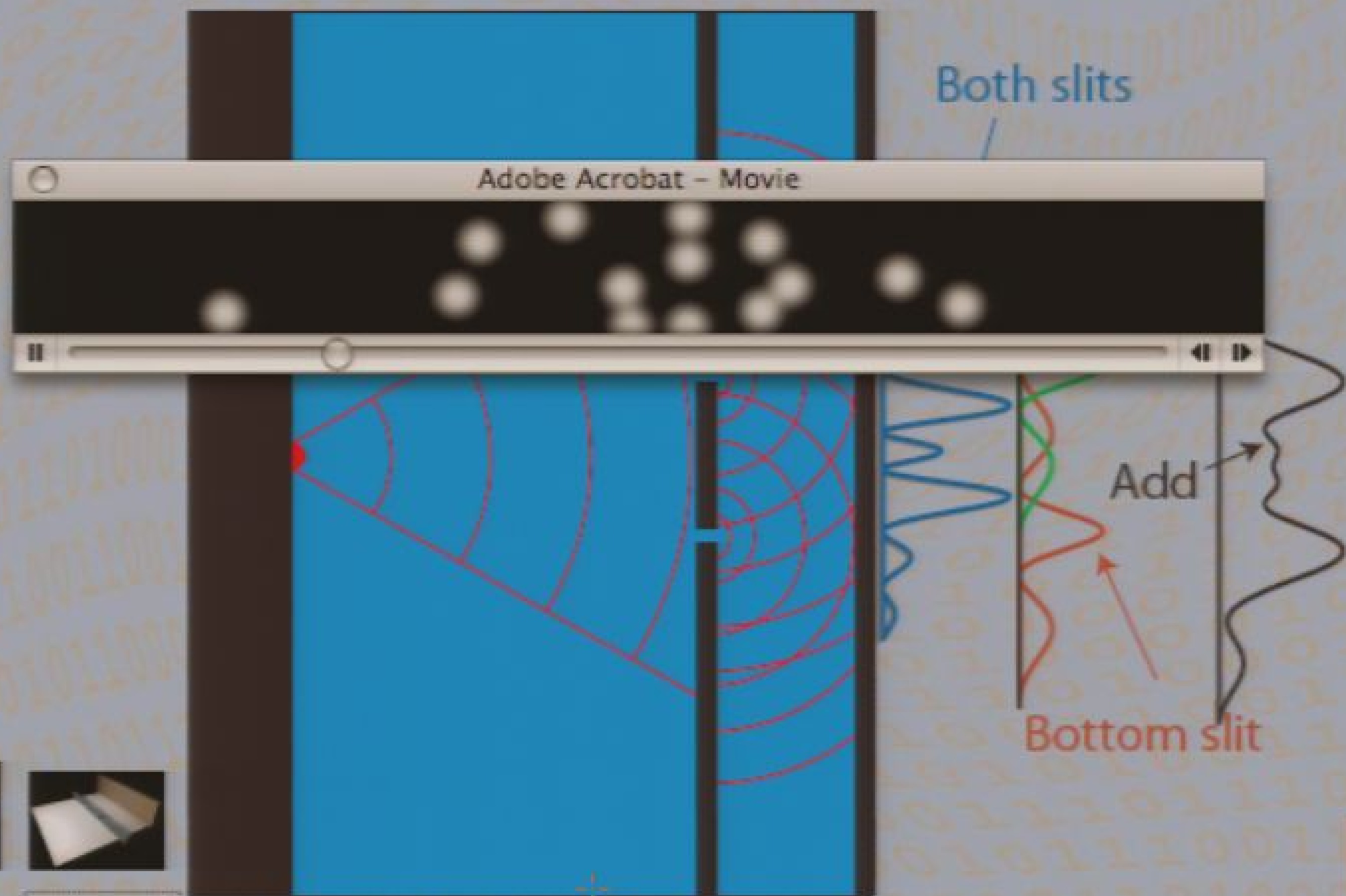
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



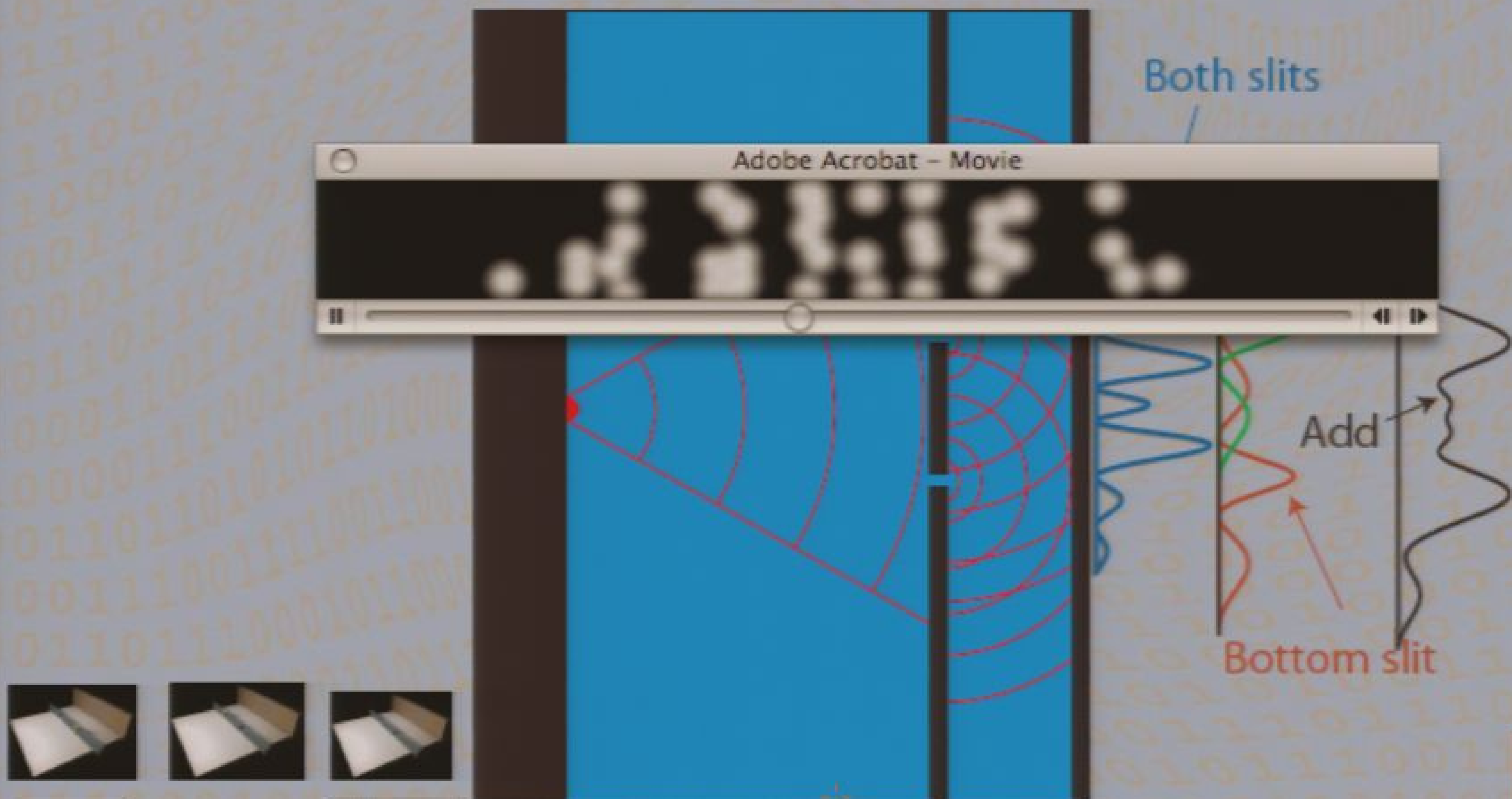
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



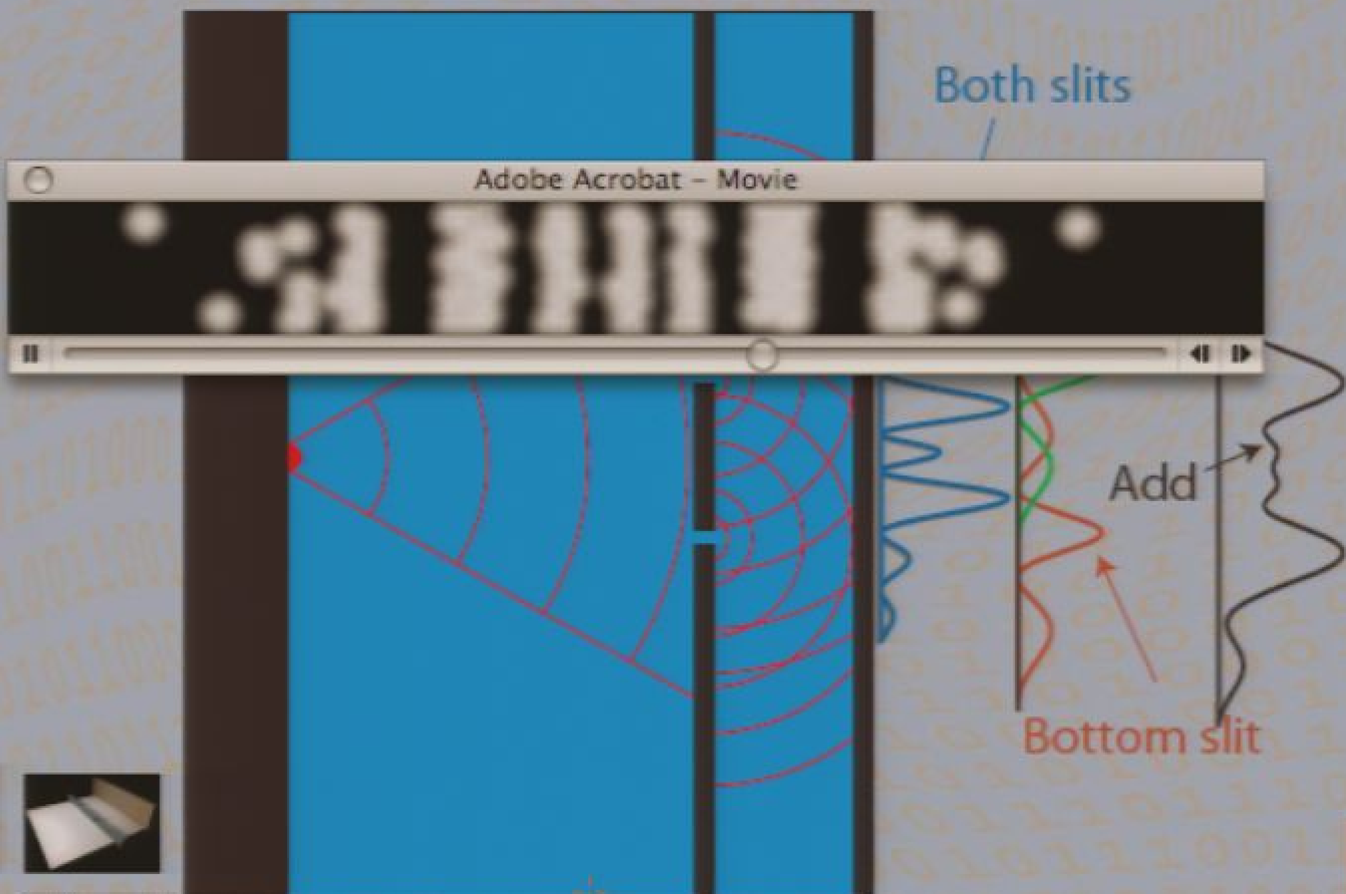
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



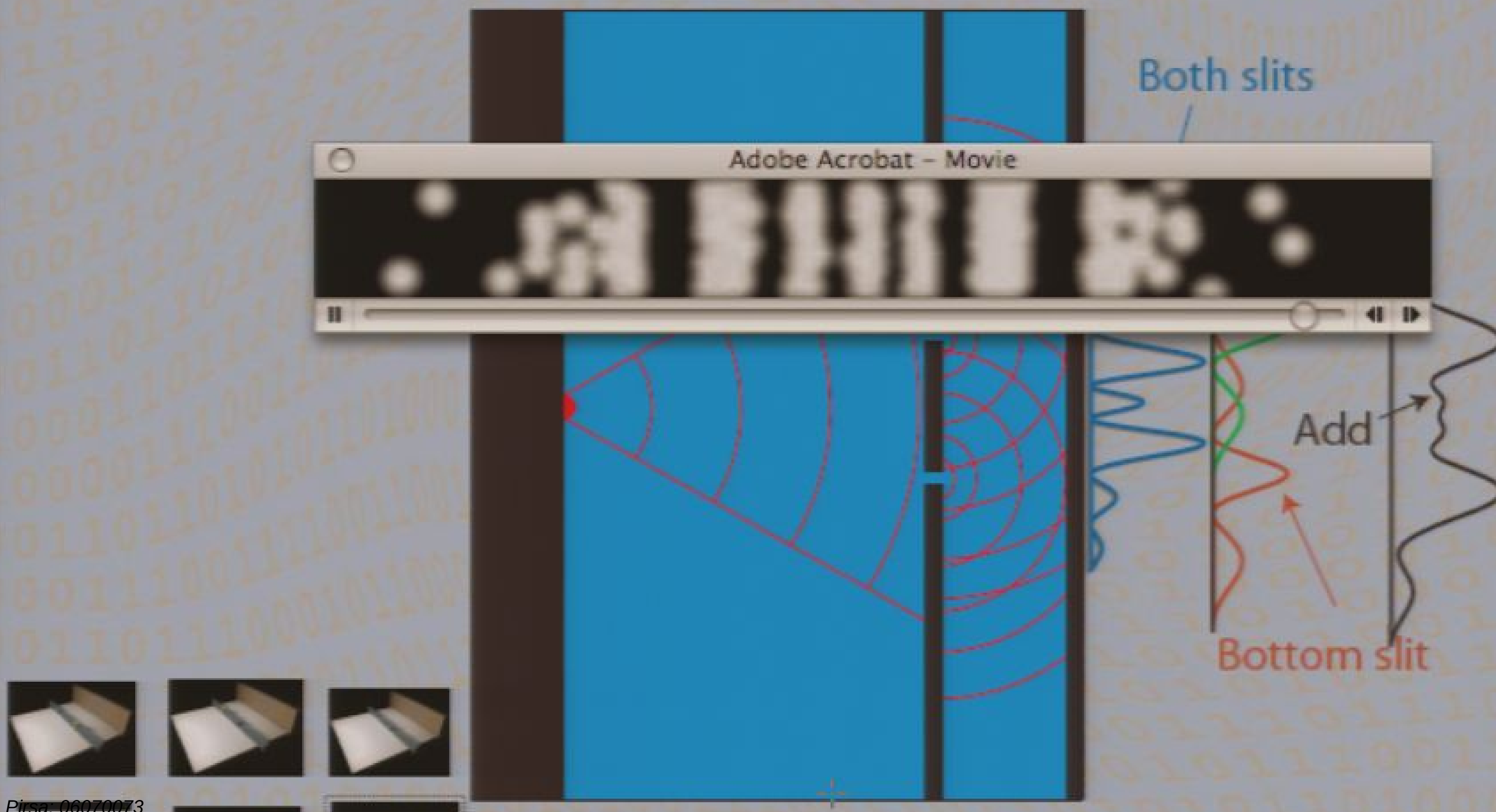
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



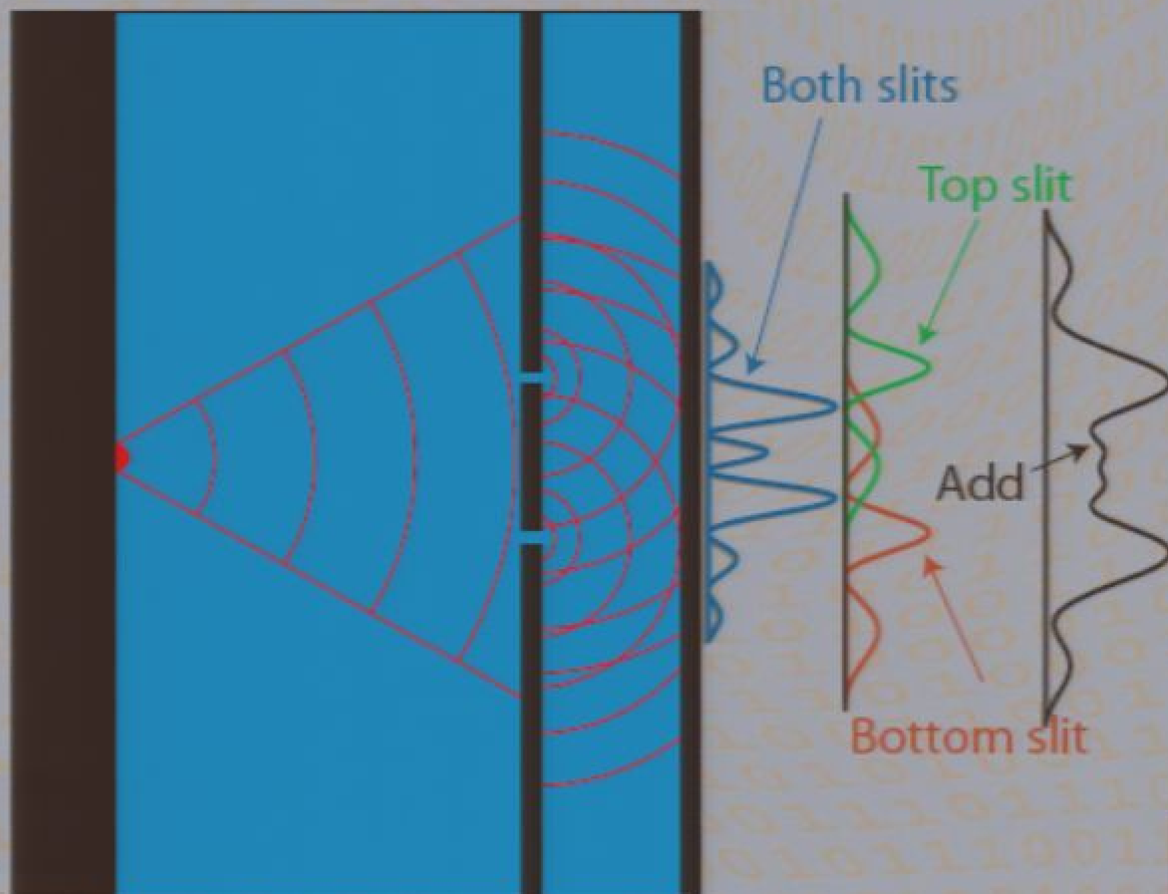
Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

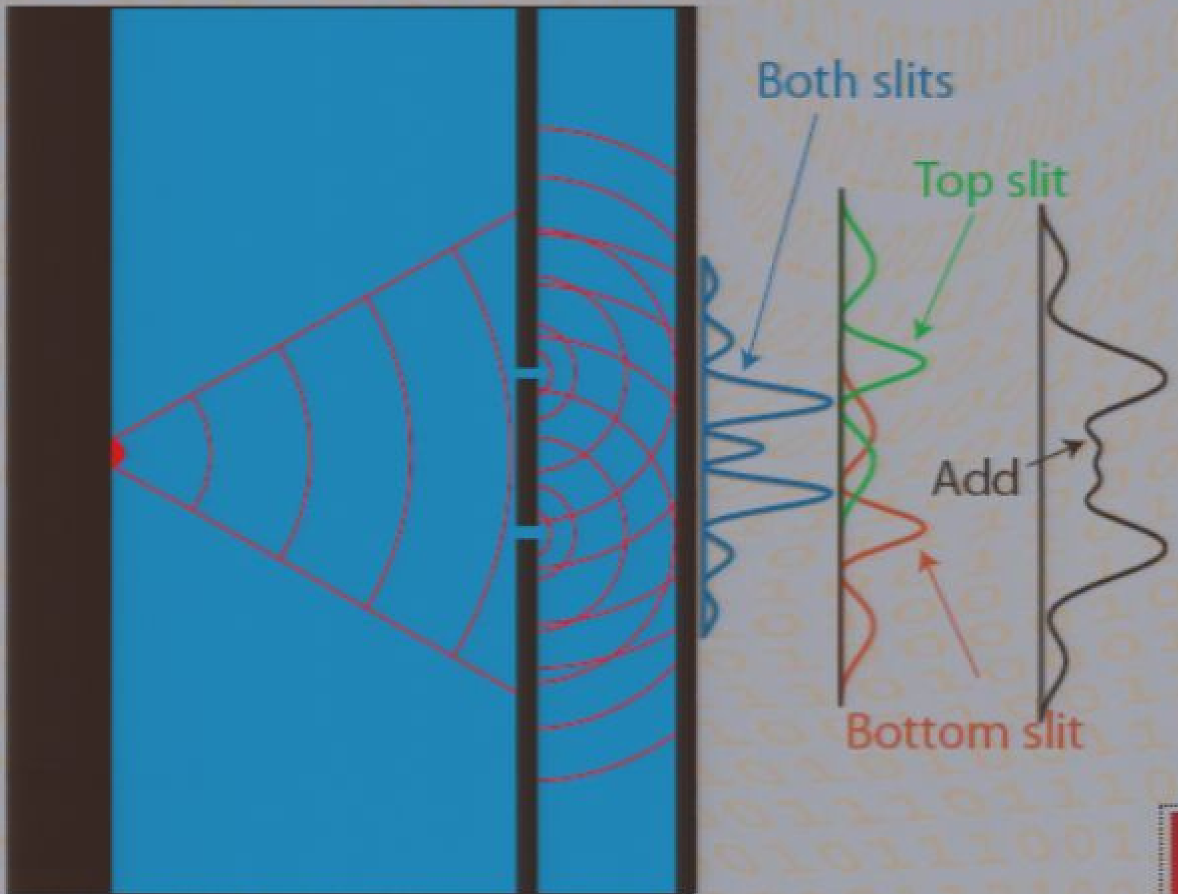


Basics of Quantum Mechanics

A coherent li[...]rough 2 slits, the result of [...]he final result when both sl[...]

Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



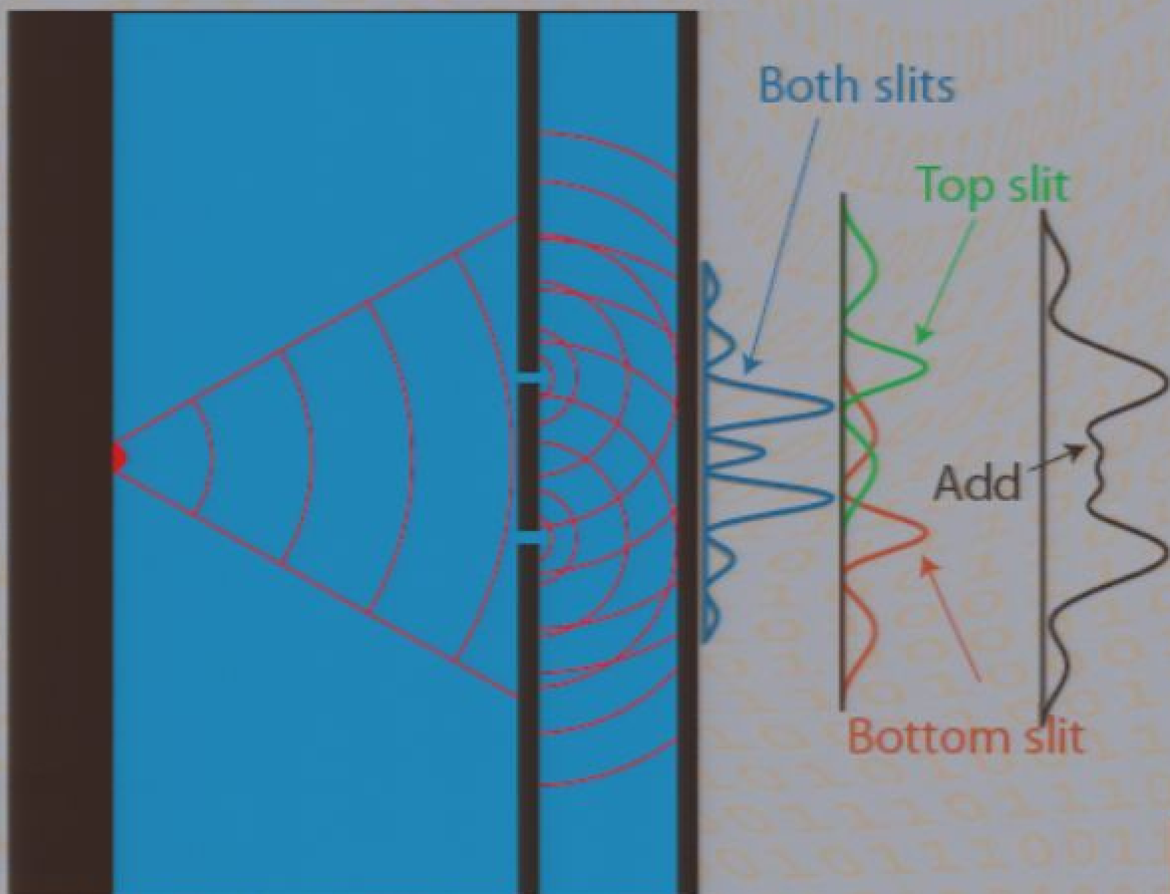
Two properties of Quantum Mechanics:

- Quantum systems behave both as waves and particles. These particles can be at more than one place at once.

- Looking at quantum systems always leaves a fingerprint.

Basics of Quantum Mechanics

A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

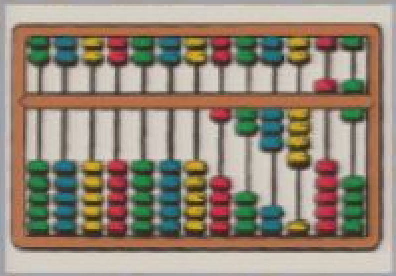


Two properties of Quantum Mechanics:

- Quantum systems behave both as waves and particles. These particles can be at more than one place at once.

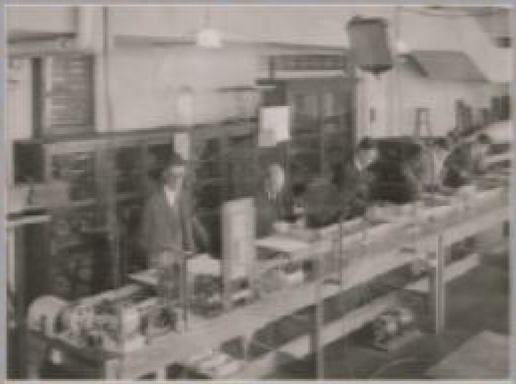
- Looking at quantum systems always leaves a fingerprint.

Early computing devices



Abacus

Babbage
Analytical engine



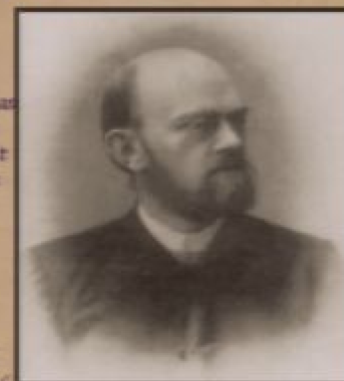
MIT's mechanical mind

Mathematical Problems

Lecture delivered before the International Congress of Mathematicians at Paris in 1900

By Professor David Hilbert

2. The compatibility of the arithmetical axioms



When we are engaged in investigating the foundations of a science, we must set up a system of axioms which contains an exact and complete description of the relations subsisting between the elementary ideas of that science. The axioms so set up are at the same time the definitions of those elementary ideas; and no statement within the realm of the science whose foundation we are testing is held to be correct unless it can be derived from those axioms by means of a finite number of logical steps. Upon closer consideration the question arises: Whether, in any way, certain statements of single axioms depend upon one another, and whether the axioms may not therefore contain certain parts in common, which must be isolated if one wishes to arrive at a system of axioms that shall be altogether independent of one another.

But above all I wish to designate the following as the most important among the numerous questions which can be asked with regard to the axioms: To prove that they are not contradictory, that is, that a definite number of logical steps based upon them can never lead to contradictory results.

In geometry, the proof of the compatibility of the axioms can be effected by constructing a suitable field of numbers, such that analogous relations between the numbers of this field correspond to the geometrical axioms. Any contradiction in the deductions from the geometrical axioms must thereupon be recognizable in the arithmetic of this field of numbers. In this way the desired proof for the compatibility of the geometrical axioms is made to depend upon the theorem of the compatibility of the arithmetical axioms.

On the other hand a direct method is needed for the proof of the compatibility of the arithmetical axioms. The axioms of arithmetic are essentially nothing else than the known rules of calculation, with the addition of the axiom of continuity. I recently collected them; and in so doing replaced the axiom of continuity by two simpler axioms, namely, the well-known axiom of Archimedes, and a new axiom essentially as follows: that numbers form a system of things which is capable of no further extension, as long as all the other axioms hold (axiom of completeness). I am convinced that it must be possible to find a direct proof for the compatibility of the arithmetical axioms, by means of a careful study and suitable modification of the known methods of reasoning in the theory of irrational numbers.

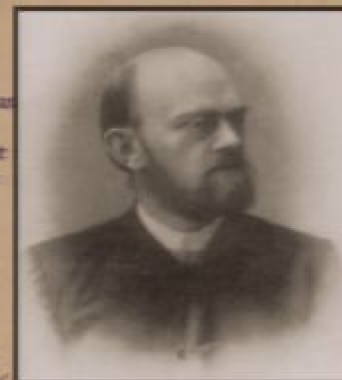
To show the significance of the problem from another point of view, I add the following observation: If contradictory attributes be assigned to a concept, I say, that mathematically the concept does not exist. So, for example, a real number whose square is -1 does not exist mathematically. But if it can be proved that the attributes assigned to the concept can never lead to a contradiction by the application of a finite number of logical processes, I say that the mathematical existence of the concept (for example, of a number or a function which satisfies certain conditions) is thereby proved. In the case before us, where we are concerned with the axioms of real numbers in arithmetic, the proof of the compatibility of the axioms is at the same time the proof of the mathematical existence of the complete system of real numbers or of the continuum. Indeed, when the proof for the compatibility of the axioms shall be fully accomplished, the doubts which have been expressed occasionally as to the existence of the complete system of real numbers will become totally groundless. The totality of real numbers, i. e., the continuum according to the point of view just indicated, is not the totality of all possible series in decimal fractions, or of all possible laws according to which the elements of a fundamental sequence may proceed. It is rather a system of things whose mutual relations are governed by the axioms set up and for which all propositions, and only those, are true which can be derived from the axioms by a finite number of logical processes. In my opinion, the concept of the continuum is strictly logically tenable in this sense only. It seems to me, indeed, that this corresponds best also to what experience and intuition tell us. The concept of the continuum or even that of the system of all functions exists, then, in exactly the same sense as the system of integral, rational numbers, for example, or as Cantor's higher classes of numbers and cardinal numbers. For I am convinced that the existence of the latter, just as that of the continuum, can be proved in the sense I have described; unlike the system of all cardinal numbers or of all Cantor's alephs, for which, as may be shown, a system of axioms, compatible in my sense, cannot be set up. Either of these systems is, therefore, according to my terminology, mathematically non-existent.

Mathematical Problems

Lecture delivered before the International Congress of Mathematicians at Paris in 1900

By Professor David Hilbert

2. The compatibility of the arithmetical axioms



When we are engaged in investigating the foundations of a science, we must set up a system of axioms which contains an exact and complete description of the relations subsisting between the elementary ideas of that science. The axioms so set up are at the same time the definitions of those elementary ideas; and no statement within the realm of the science whose foundation we are testing is held to be correct unless it can be derived from those axioms by means of a finite number of logical steps. Upon closer consideration the question arises: Whether, in any way, certain statements of single axioms depend upon one another, and whether the axioms may not therefore contain certain parts in common, which must be isolated if one wishes to arrive at a system of axioms that shall be altogether independent of one another.
But above all I wish to designate the following as the most important among the numerous questions which can be asked with regard to the axioms: To prove that they are not contradictory, that is, that a definite number of logical steps based upon them can never lead to contradictory results.
In geometry, the proof of the compatibility of the axioms can be effected by constructing a suitable field of numbers, such that analogous relations between the numbers of this field correspond to the geometrical axioms. Any contradiction in the deductions from the geometrical axioms must thereupon be recognizable in the arithmetic of this field of numbers. In this way the desired proof for the compatibility of the geometrical axioms is made to depend upon the theorem of the compatibility of the arithmetical axioms.
On the other hand a direct method is needed for the proof of the compatibility of the arithmetical axioms. The axioms of arithmetic are essentially nothing else than the known rules of calculation, with the addition of the axiom of continuity. I recently collected them, and in so doing replaced the axiom of continuity by two simpler axioms, namely, the well-known axiom of Archimedes, and a new axiom essentially as follows: that numbers form a system of things which is capable of no further extension, as long as all the other axioms hold (axiom of completeness). I am convinced that it must be possible to find a direct proof for the compatibility of the arithmetical axioms, by means of a careful study and suitable modification of the known methods of reasoning in the theory of irrational numbers.
To show the significance of the problem from another point of view, I add the following observation: If contradictory attributes be assigned to a concept, I say, that mathematically the concept does not exist. So, for example, a real number whose square is -1 does not exist mathematically. But if it can be proved that the attributes assigned to the concept can never lead to a contradiction by the application of a finite number of logical processes, I say that the mathematical existence of the concept (for example, of a number or a function which satisfies certain conditions) is thereby proved. In the case before us, where we are concerned with the axioms of real numbers in arithmetic, the proof of the compatibility of the axioms is at the same time the proof of the mathematical

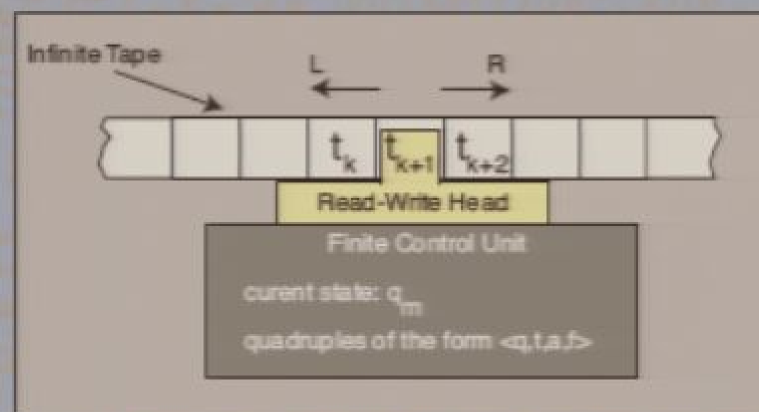
This statement is false

and intuition tell us. The concept of the continuum or even that of the system of all functions exists, then, in exactly the same sense as the system of integral, rational numbers, for example, or as Cantor's higher classes of numbers and cardinal numbers. For I am convinced that the existence of the latter, just as that of the continuum, can be proved in the sense I have described; unlike the system of all cardinal numbers or of all Cantor's alephs, for which, as may be shown, a system of axioms, compatible in my sense, cannot be set up. Either of these systems is, therefore, according to my terminology, mathematically non-existent.

Turing machines

Turing

Church



Turing machine

"We can only see
a short distance ahead,
but we can see plenty there
that needs to be done."

Alan Turing

Complexity theory

Goal: asses the amount of ressources to solve problems

- Adding: $\underbrace{748230}+3802=752032$

  Scale is number of digit of input

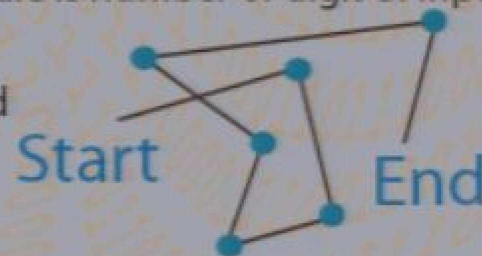
- Factor in product of primes: $\underbrace{54029}=97\times557$

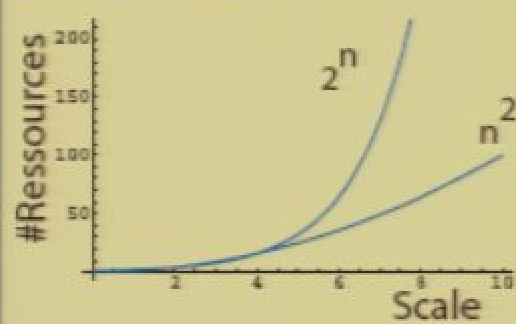
  Scale is number of digit of input

- Travelling salesperson:

  Find the shortest route from Start to End

  Scale is number of cities





- Hard problems: exponential amount of ressources
- Easy problems: polynomial amount of ressources

Strong Church Turing principle:

no machine can turn a hard problem into an easy one

Quantum Factoring

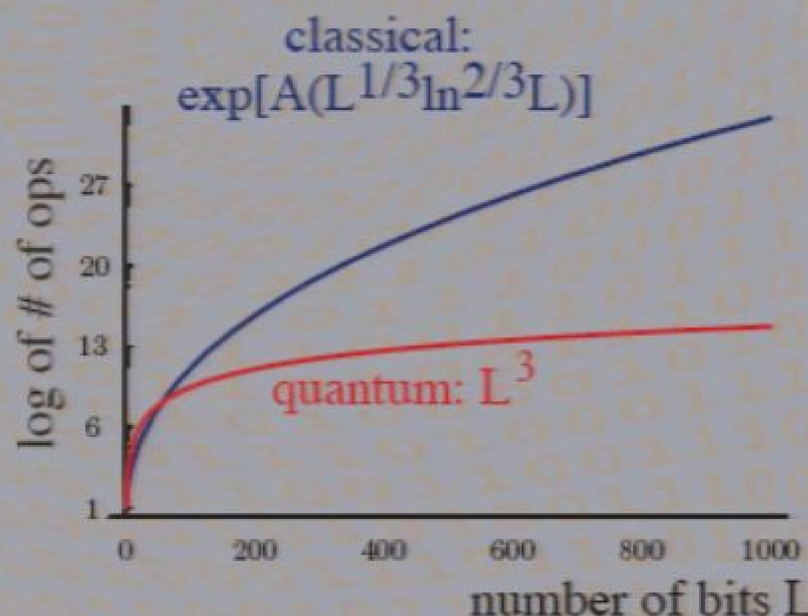

Peter Shor

(Shor, IEEE Press 1994)

$n=pq \quad (L = \ln n)$

Today the fastest classical computers can factor number with ~150 digits

Quantum algorithm
# of gates ~$12L^3$
# of qubits ~$5L$



RSA Data Security.
A Security Dynamics Company

A classical computer in a nutshell

- Classical bits of information are encoded in physical systems which has two states 0 and 1

...110 01000 11101 000... → ...001 01100 00101 010...

- Transformations are made with (universal) gates

Not Gate $1 \to 0$ or $0 \to 1$

And Gate

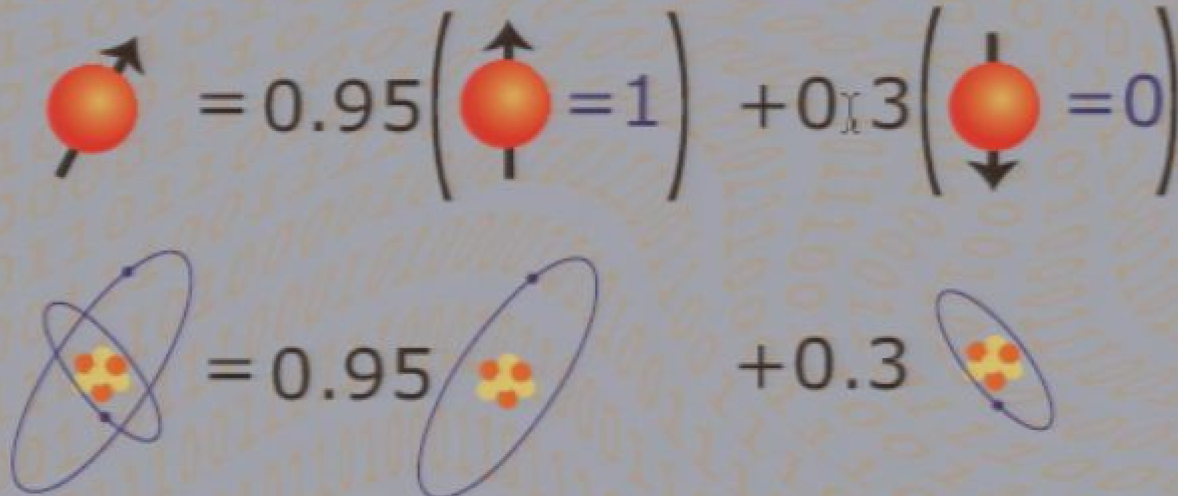
in		out
0	0	0
1	0	0
0	1	0
1	1	1

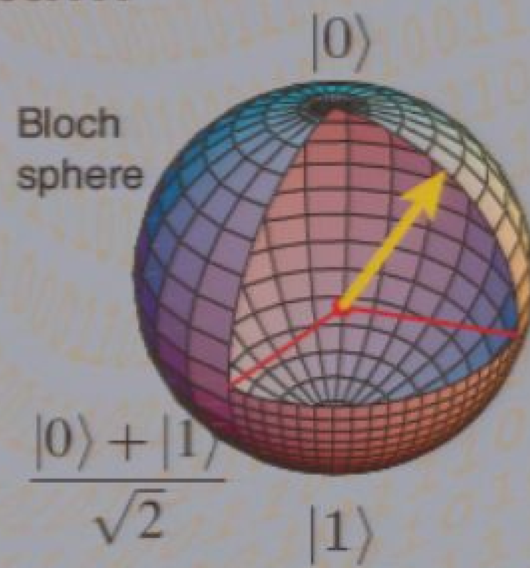
Input 1
Input 2 → Ouput

Input 1 And Input 2

A quantum computer in a nutshell

Quantum bits (qubits) are quantum systems with two levels





Universal set of operations (gates)
-generic one bit gates
-any interaction between qubits

Bits can be superposed!

A classical computer in a nutshell

- Classical bits of information are encoded in physical systems which has two states 0 and 1

...110 → ...001
01000 → 01100
11101 → 00101
000... → 010...

- Transformations are made with (universal) gates

Not Gate $1 \rightarrow 0$ or $0 \rightarrow 1$

And Gate

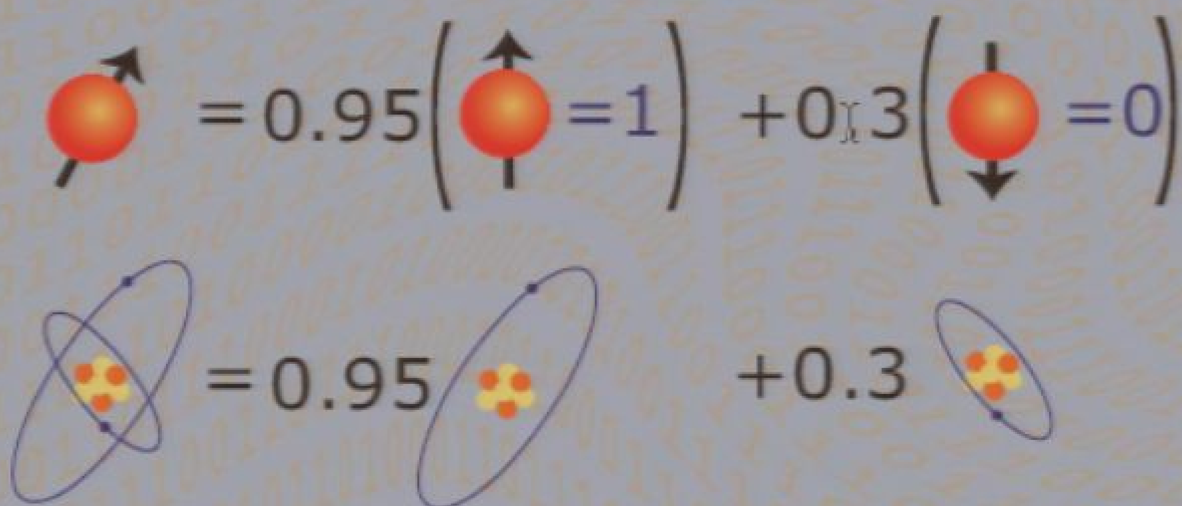
in		out
0	0	0
1	0	0
0	1	0
1	1	1

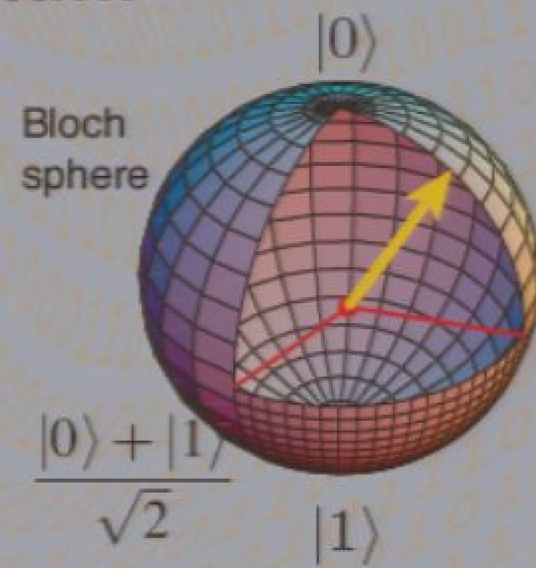
Input 1
Input 2 → Ouput

Input 1 And Input 2

A quantum computer in a nutshell

Quantum bits (qubits) are quantum systems with two levels

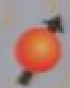




Universal set of operations (gates)
-generic one bit gates
-any interaction between qubits

Bits can be superposed!

The power of Quantum Computers

# of quantum bits	quantum states	# of classical bits
1 	0,1	$2^1 = 2$

A quantum bit
can be in two states
at the same time

We need two paramters to decribe the state

The power of Quantum Computers

# of quantum bits	quantum states	# of classical bits
1	0,1	$2^1 = 2$
2	00,01,10,11	$2^2 = 4$

Two quantum bit
can be in four states
at the same time

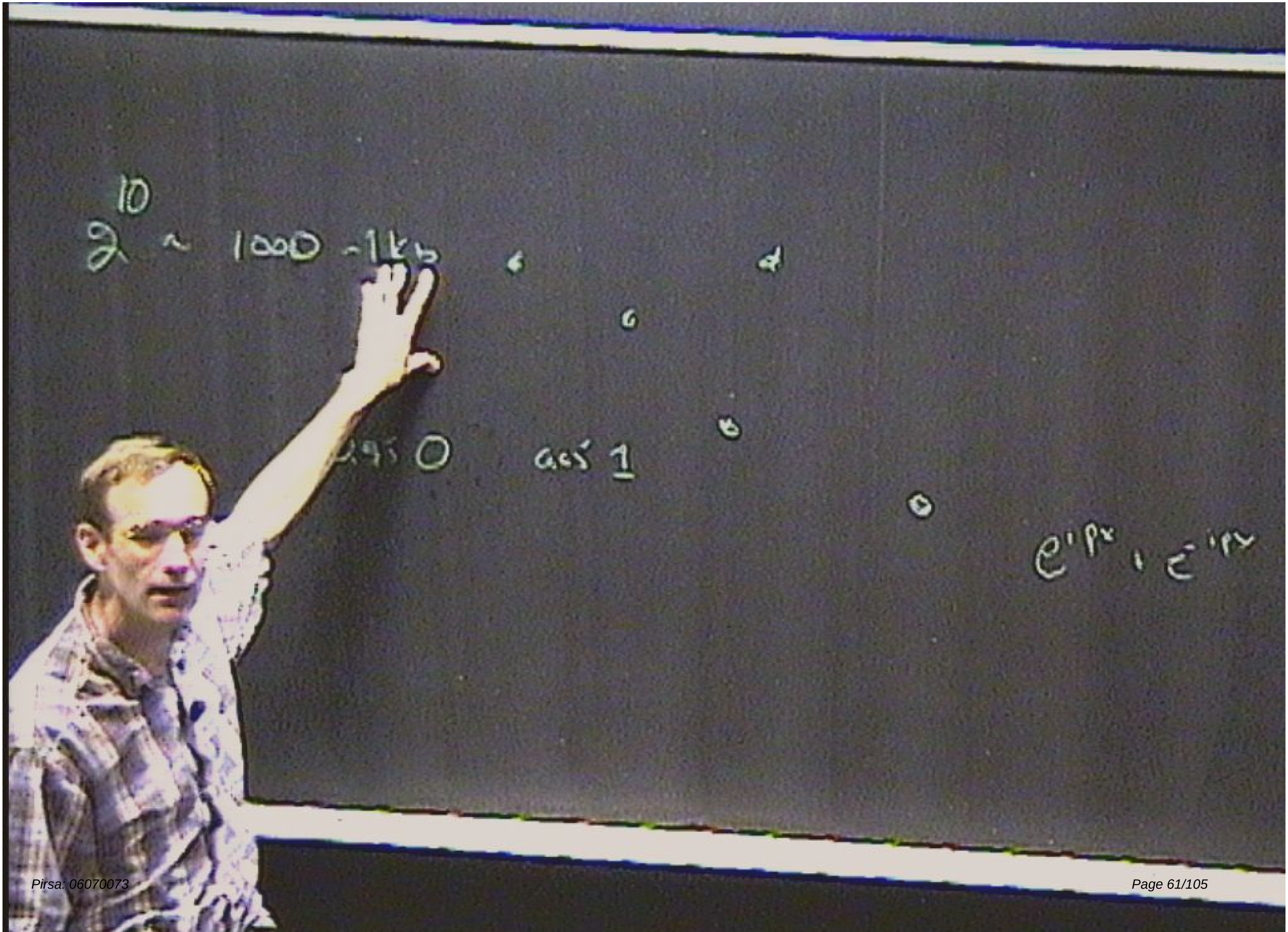
We need four paramters to decribe the state

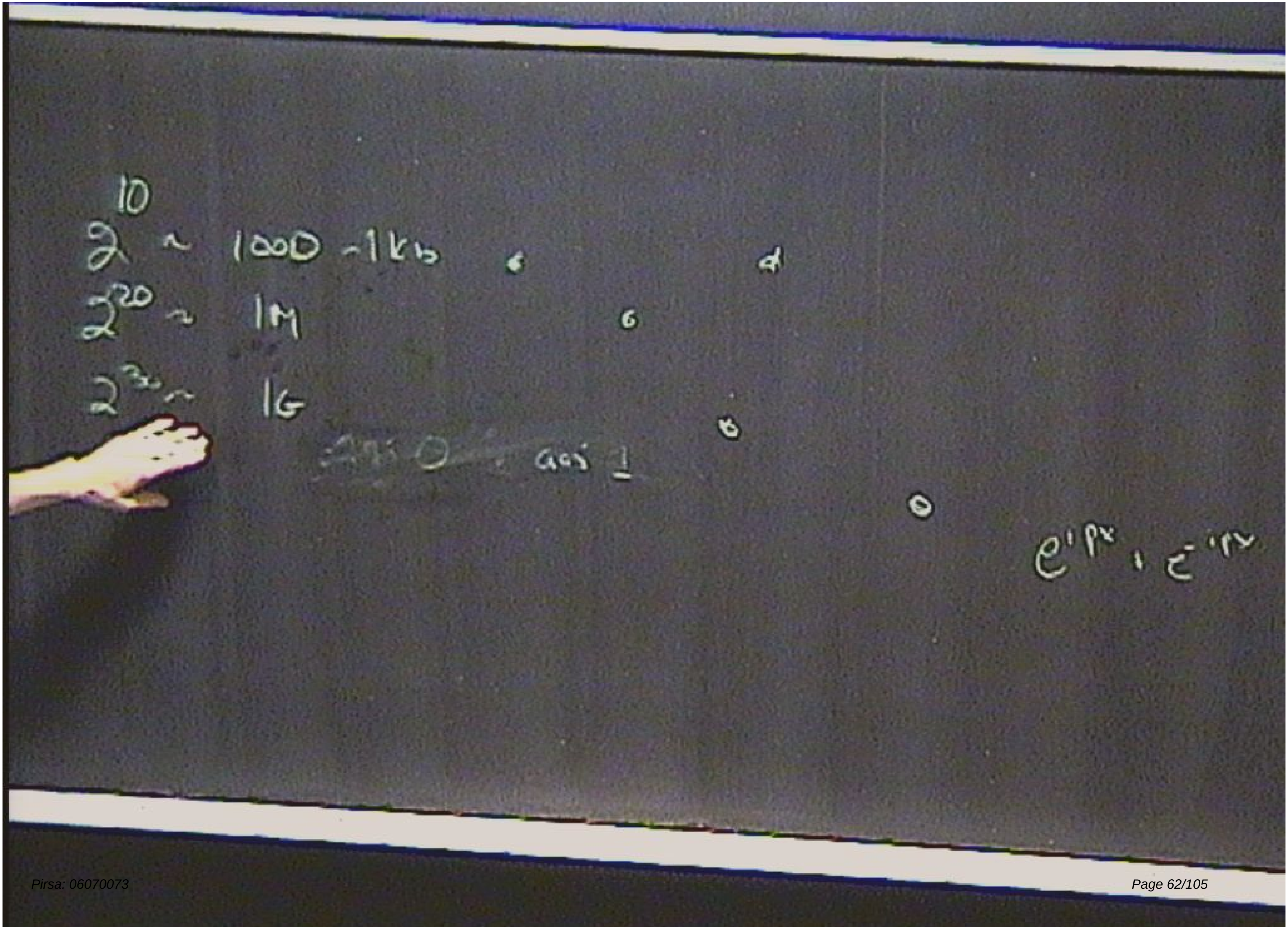
The power of Quantum Computers

# of quantum bits	quantum states	# of classical bits
1	0,1	$2^1=2$
2	00,01,10,11	$2^2=4$
3	000,001,...,111	$2^3=8$

The power of Quantum Computers

# of quantum bits	quantum states	# of classical bits
1	0,1	$2^1=2$
2	00,01,10,11	$2^2=4$
3	000,001,...,111	$2^3=8$
4	0000,0001,...,1111	$2^4=16$


2^10 ~ 1000 ~1kb
e^ipx, e^-ipx


$2^{10} \sim 1000 \sim 1$ kb
$2^{20} \sim 1M$
$2^{30} \sim 1G$
~~cos 0~~ cos 1
e^{ipx}, e^{-ipx}

$$2^{10} \sim 1000 \sim 1\,\text{kb}$$

$$2^{20} \sim 1\text{M}$$

$$2^{30} \sim 1\text{G}$$

$$2^{40} \sim 1\ \text{Terabyte}$$

e^{ipx}, e^{-ipx}

$2^{10} \sim 1000 \sim 1\,\mathrm{Kb}$

$2^{20} \sim 1\mathrm{M}$

$2^{30} \sim 1\mathrm{G}$

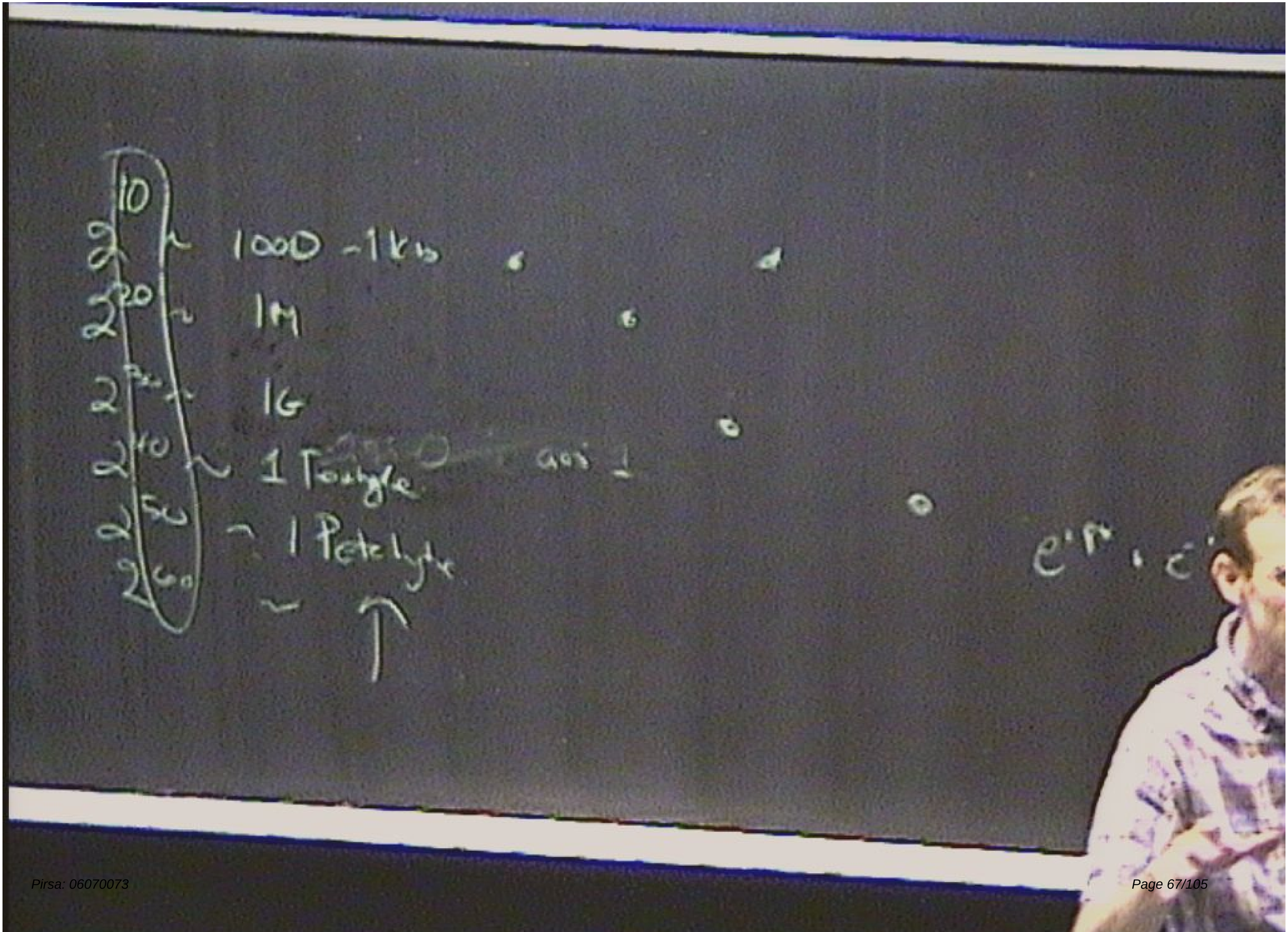
$2^{40} \sim 1$ Terabyte

$2^{50} \sim 1$ Petabyte

$2^{60} \sim$

ans 0 ans 1

$e^{ipx},\ e^{-ipx}$


10
2^10 ~ 1000 ~ 1 kb
2^20 ~ 1M
2^30 ~ 1G
2^40 ~ 1 Terabyte
2^50 ~ 1 Petabyte
2^60 ~

The power of Quantum Computers

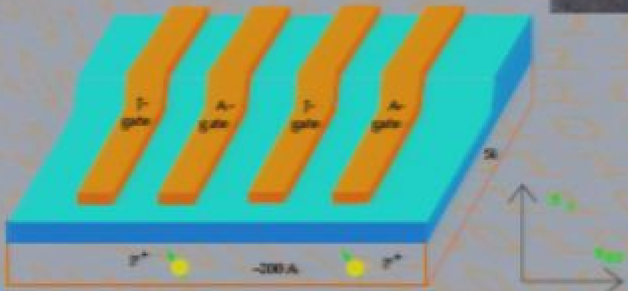
# of quantum bits	quantum states	# of classical bits
1	0,1	$2^1 = 2$
2	00,01,10,11	$2^2 = 4$
3	000,001,...,111	$2^3 = 8$
4	0000,0001,...,1111	$2^4 = 16$
⋮		⋮
10 ···	0000000000,...	$2^{10} = 1k$
20 ···	0000000000...,	$2^{20} = 1M$
30 ···	0000000000...,	$2^{30} = 1G$
40 ···	0000000000...,	$2^{40} = 1T$
50 ···	0000000000...,	$2^{50} = 1P$

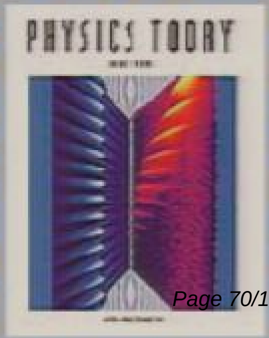
Theory vs experiment

Devices for QIP

- Atom traps
- Cavity QED
- Electron floating on helium
- Electron trapped by surface acoustic waves

- Ion trap
- Nuclear Magnetic Resonance
- Quantum dots
- Quantum optics



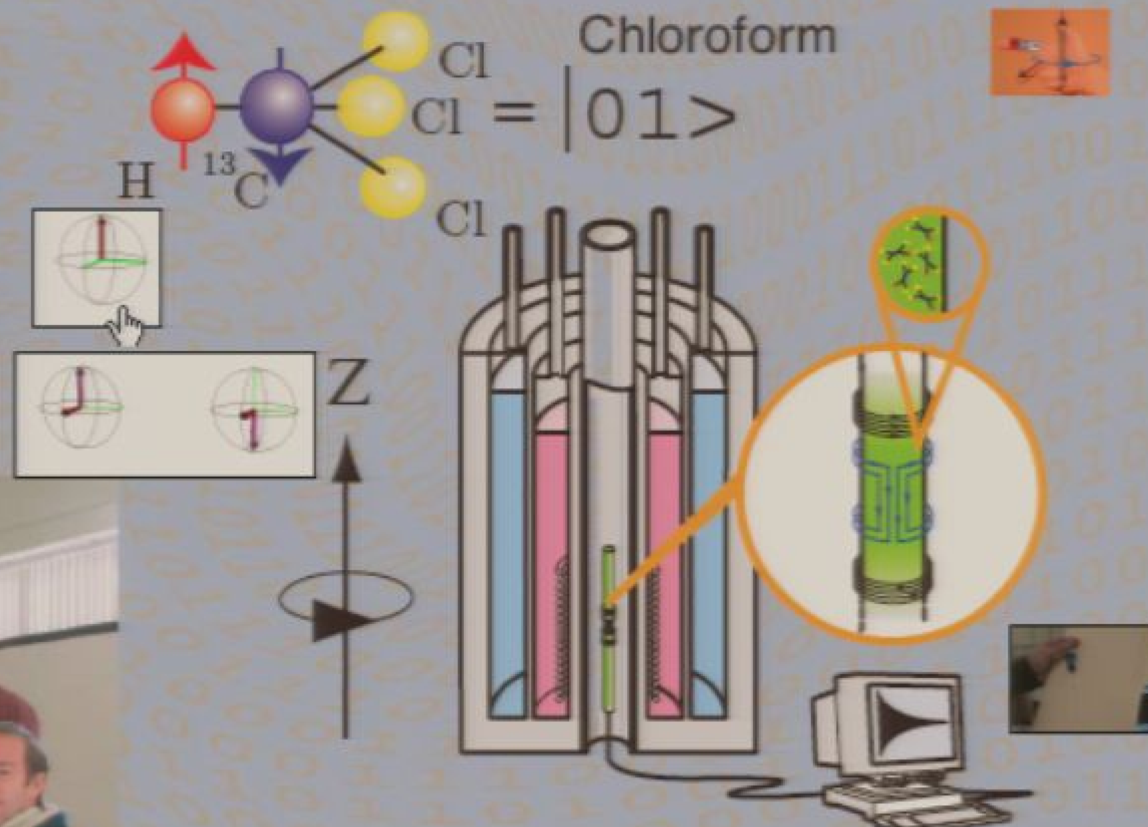


- Solid state
- Spintronics
- Superconducting Josephson junctions

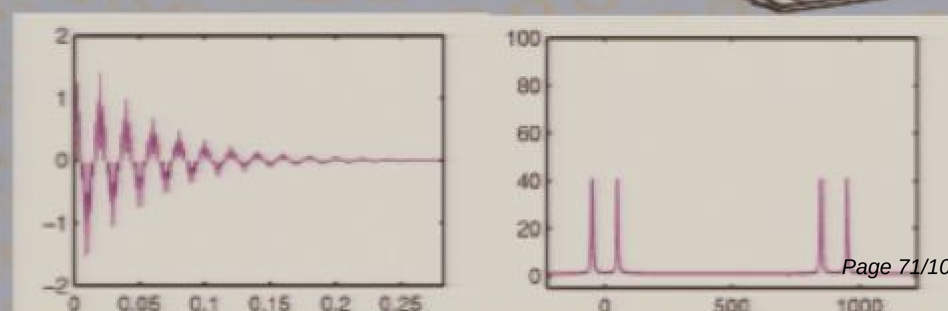
Nuclear Magnetic Resonance

Bloch

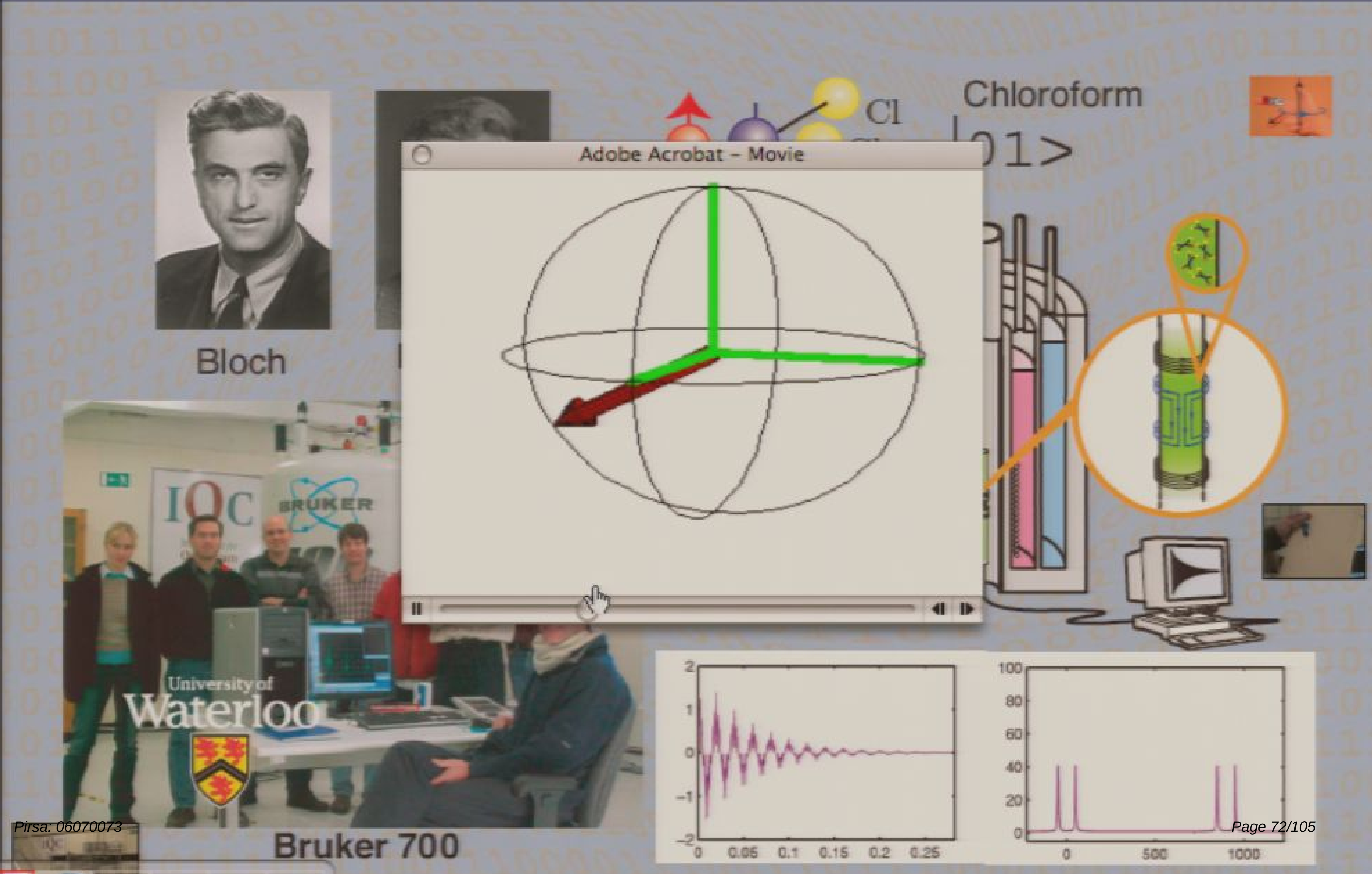
Purcell



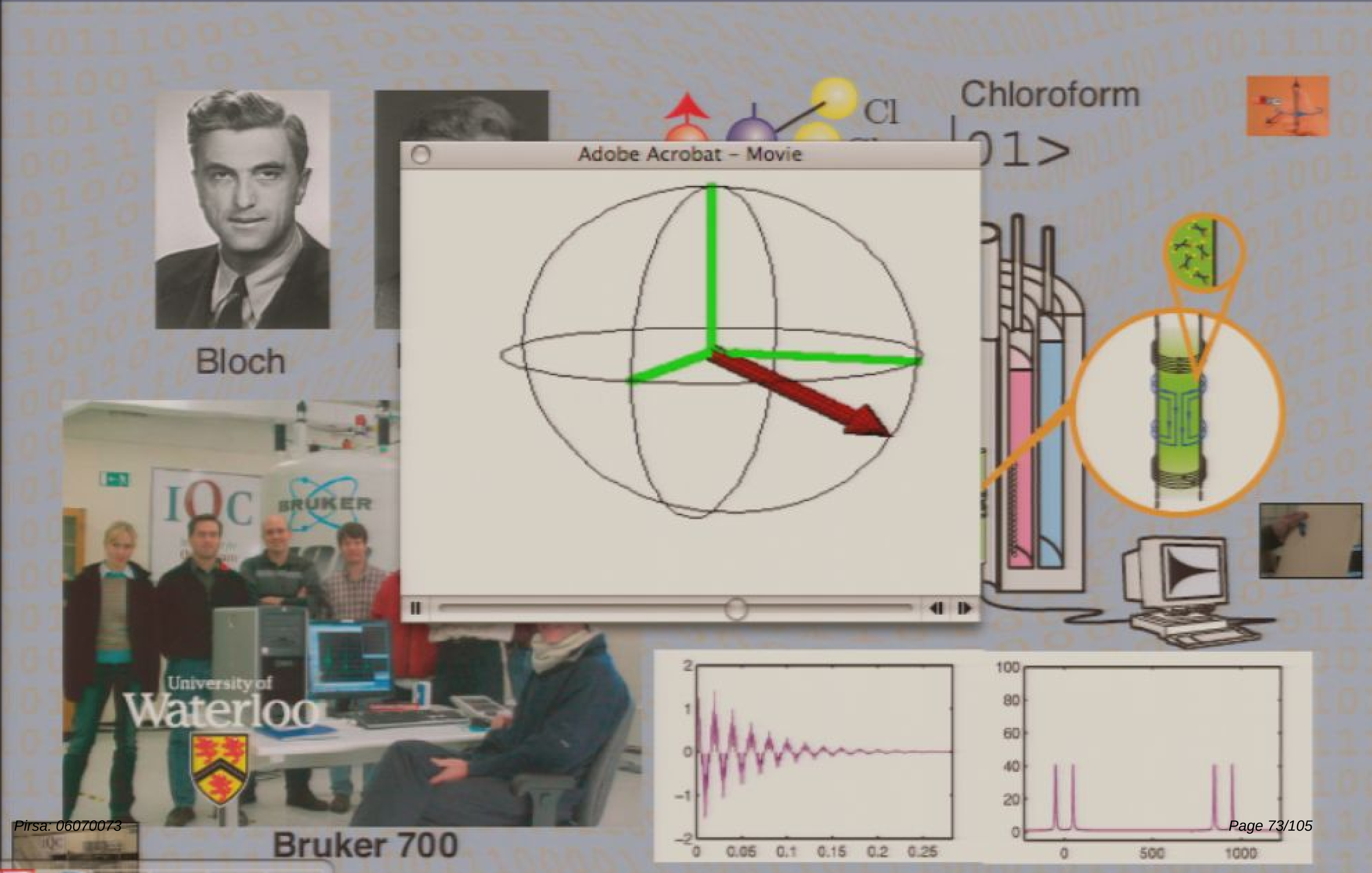
Bruker 700



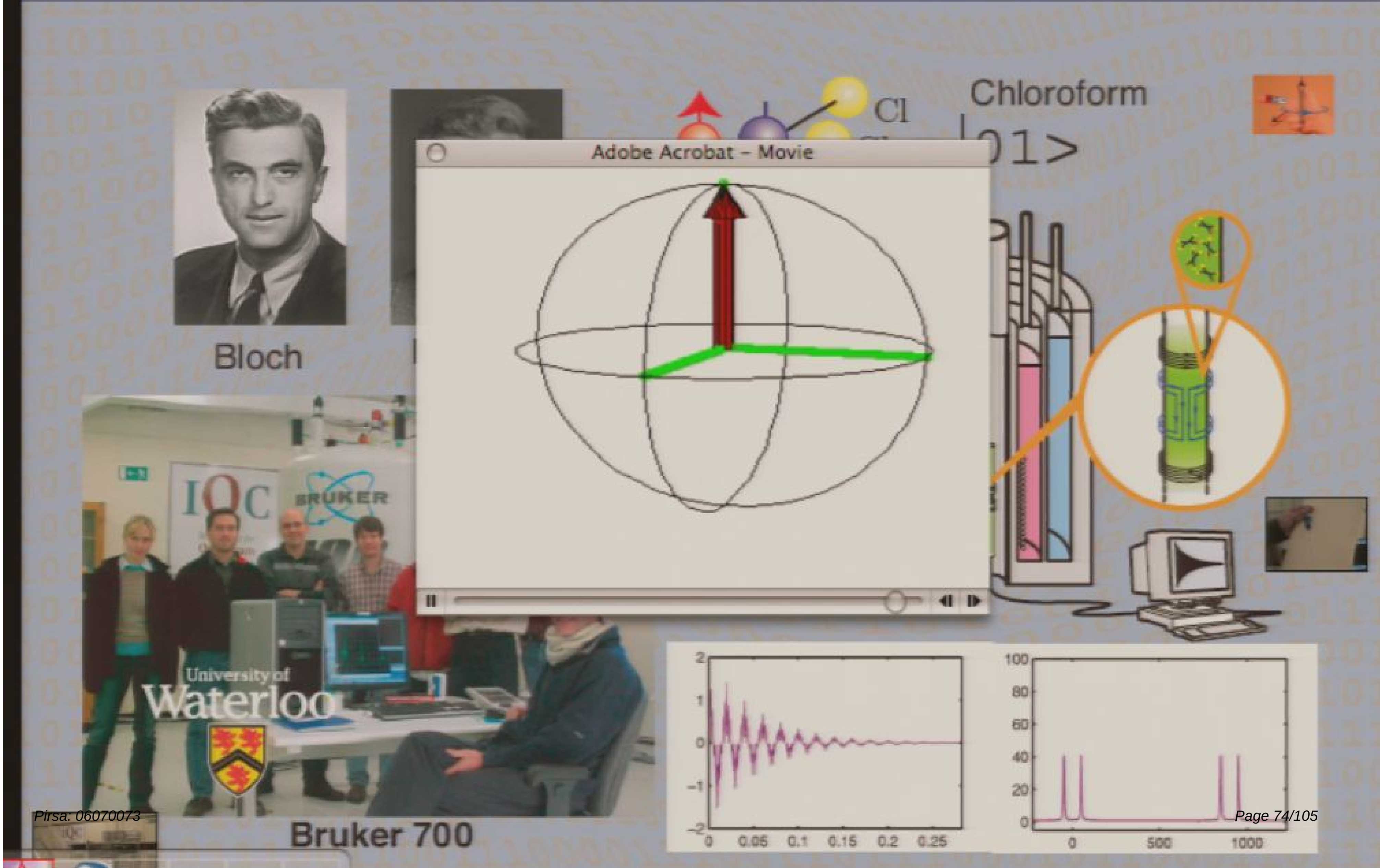
Nuclear Magnetic Resonance



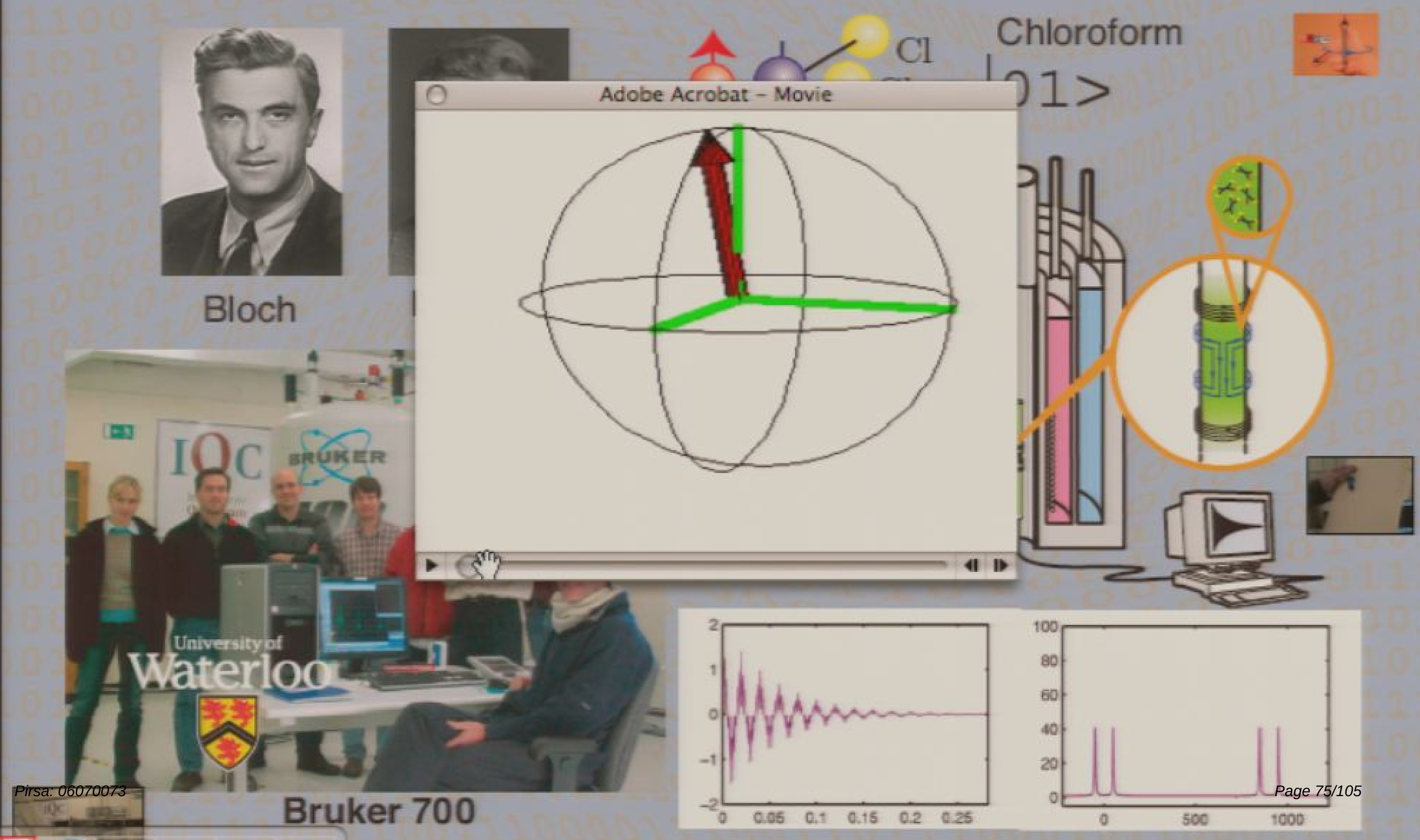
Nuclear Magnetic Resonance



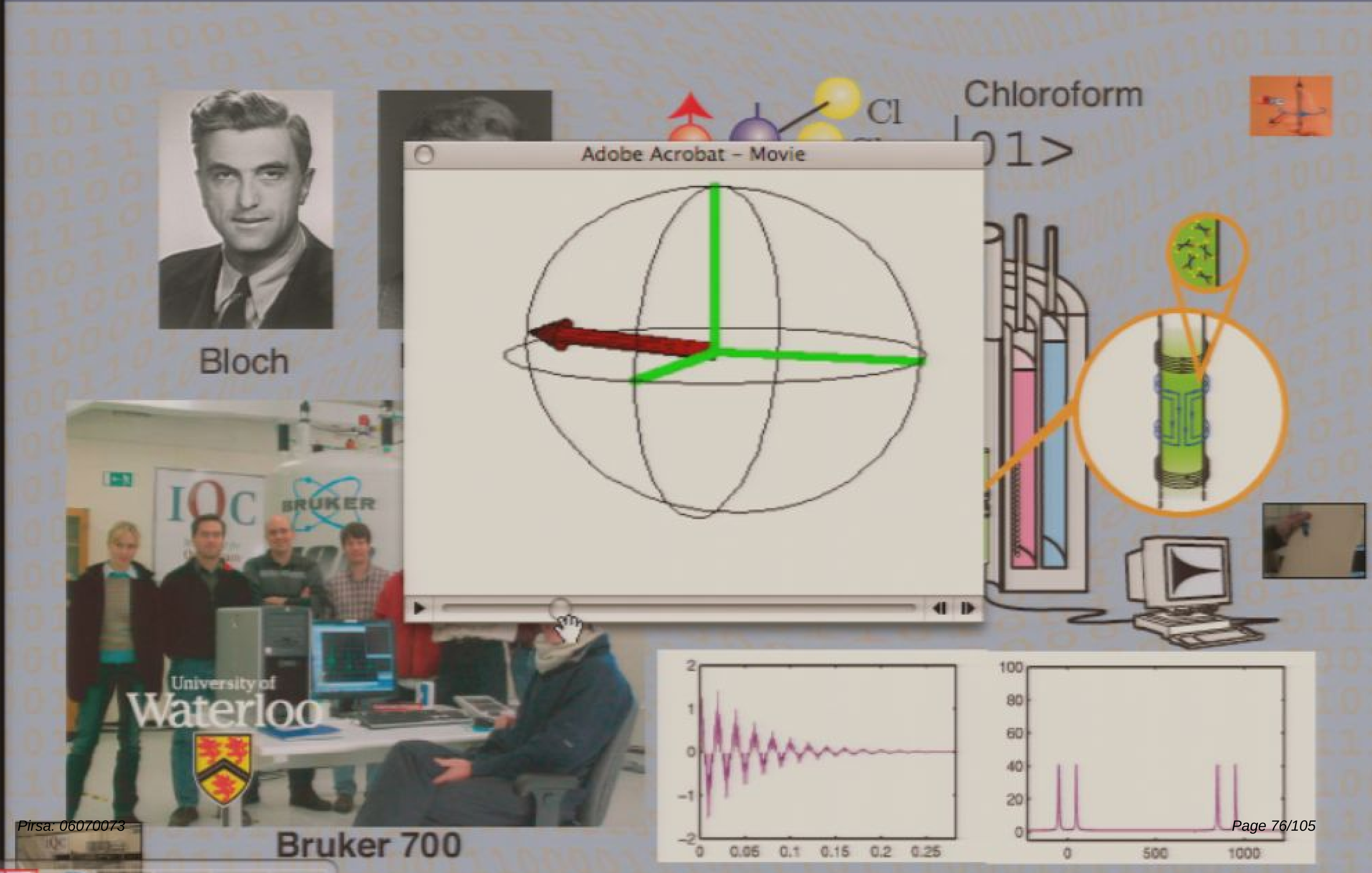
Nuclear Magnetic Resonance



Nuclear Magnetic Resonance



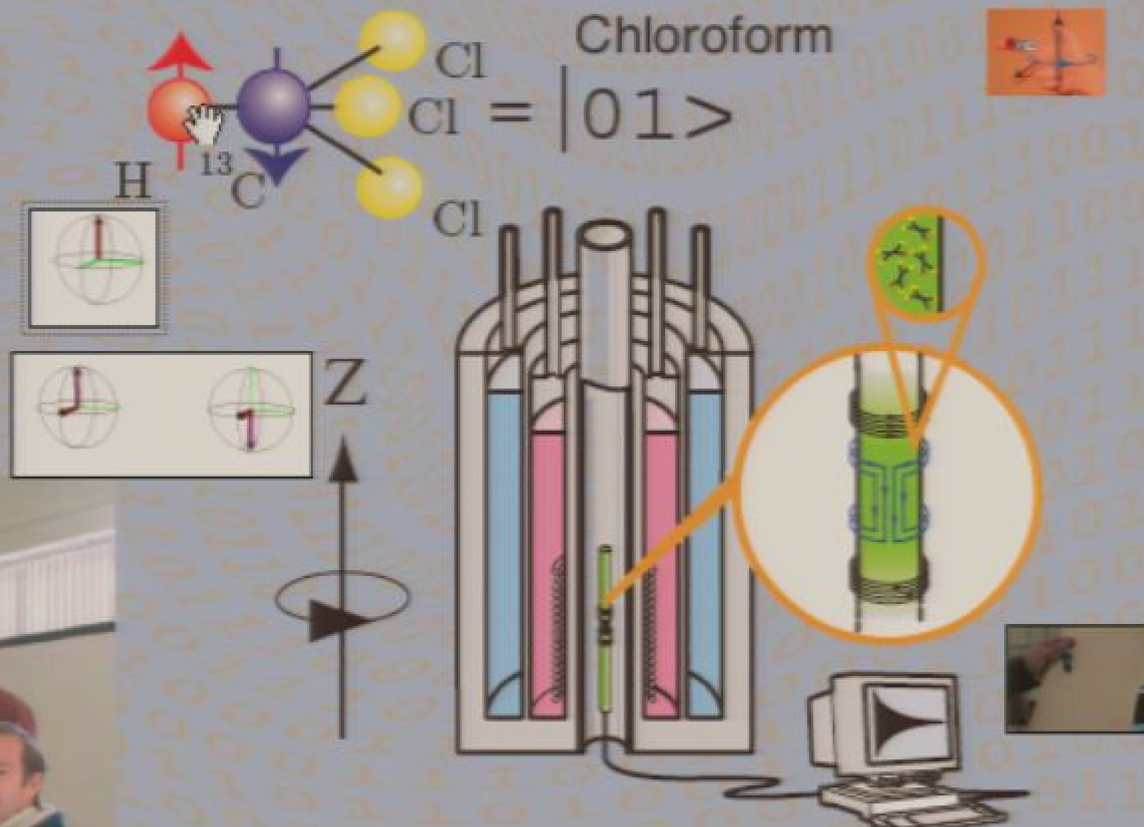
Nuclear Magnetic Resonance



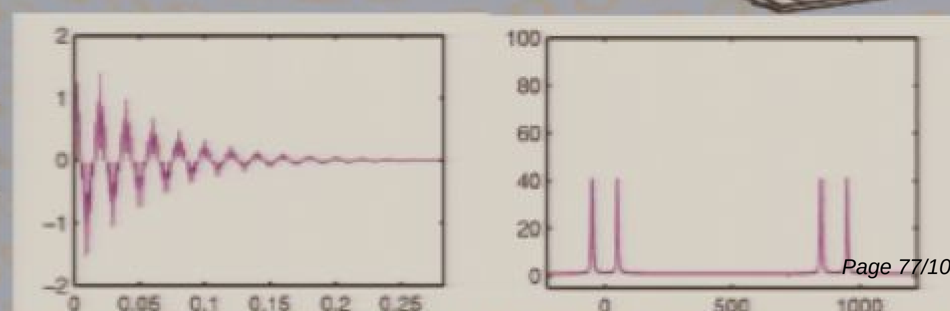
Nuclear Magnetic Resonance

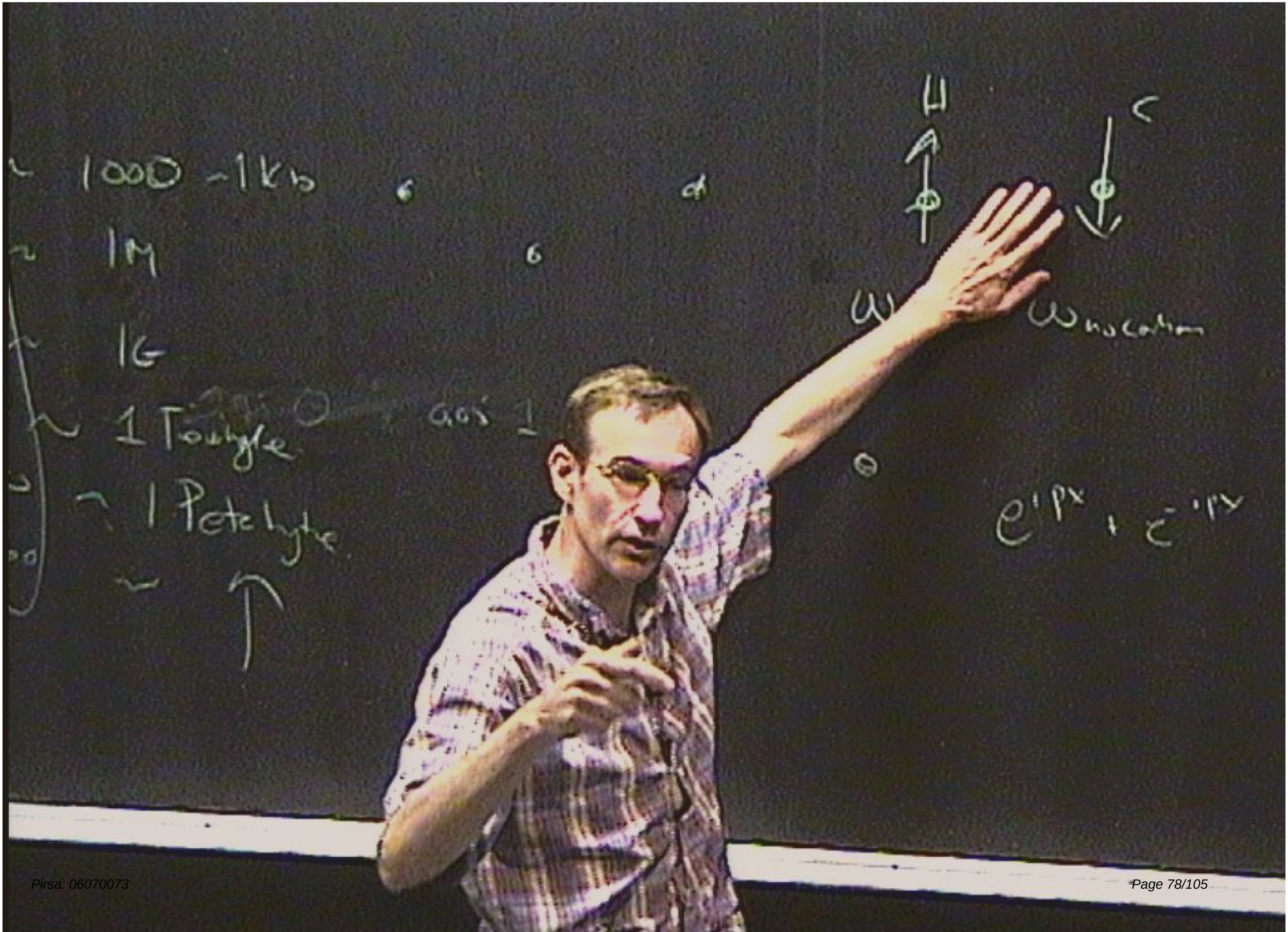
Bloch

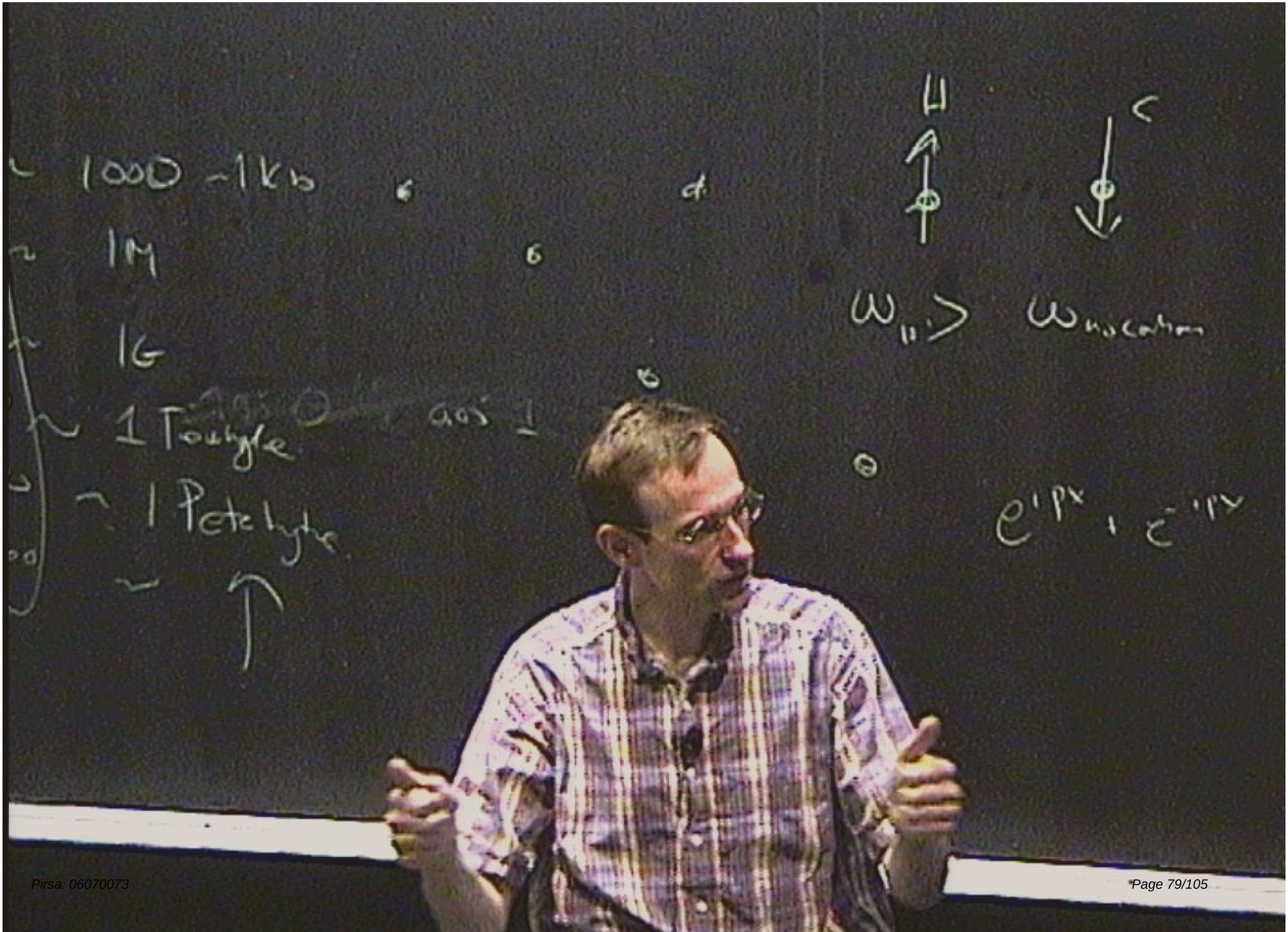
Purcell



Bruker 700




1000 ~1Kb
1M
1G
1 Petabyte

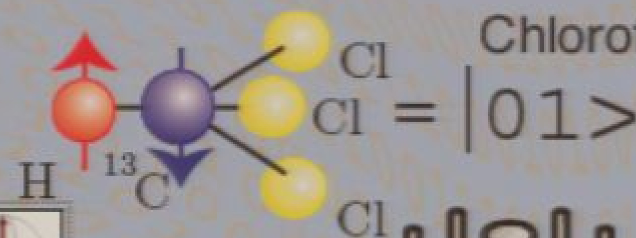

1000 ~1 Kb
1M
1G
1 Petabyte
e^{ipx} + e^{-ipx}

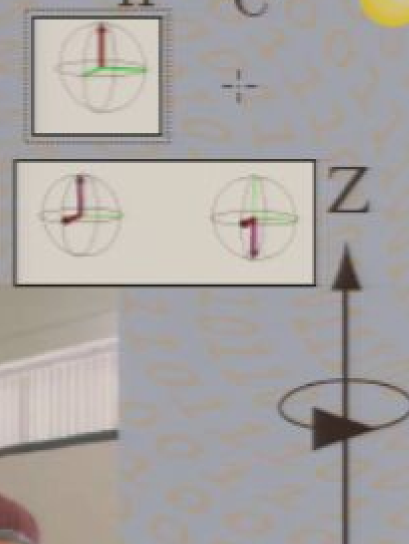
Nuclear Magnetic Resonance

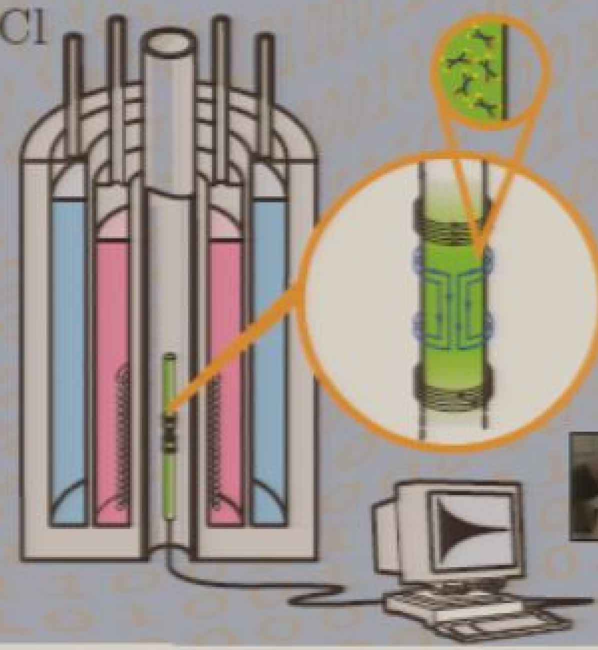
Bloch

Purcell

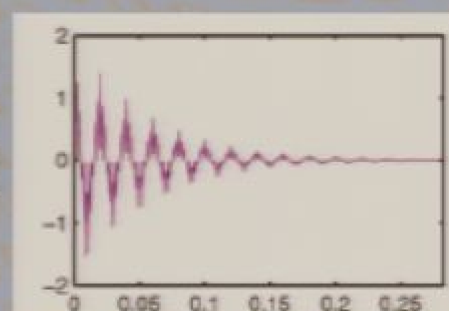
Chloroform

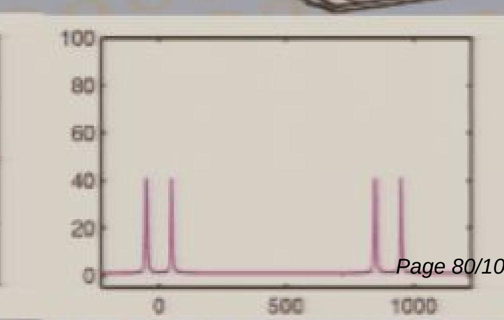






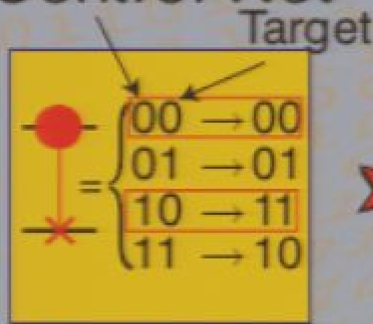
Bruker 700



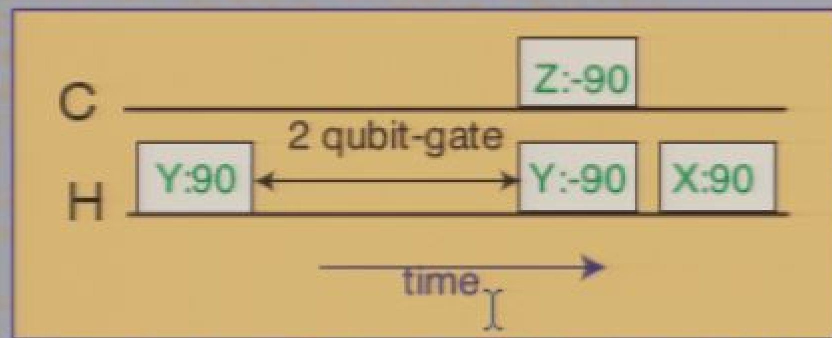


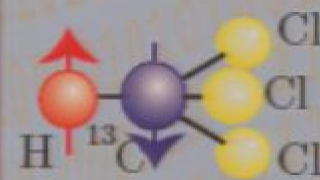
Quantum algorithms 101: the Control-NOT

Control-Not



Quantum circuit





Pre-compiler (Optimizer)

```
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
  refocus C1C2_180
```

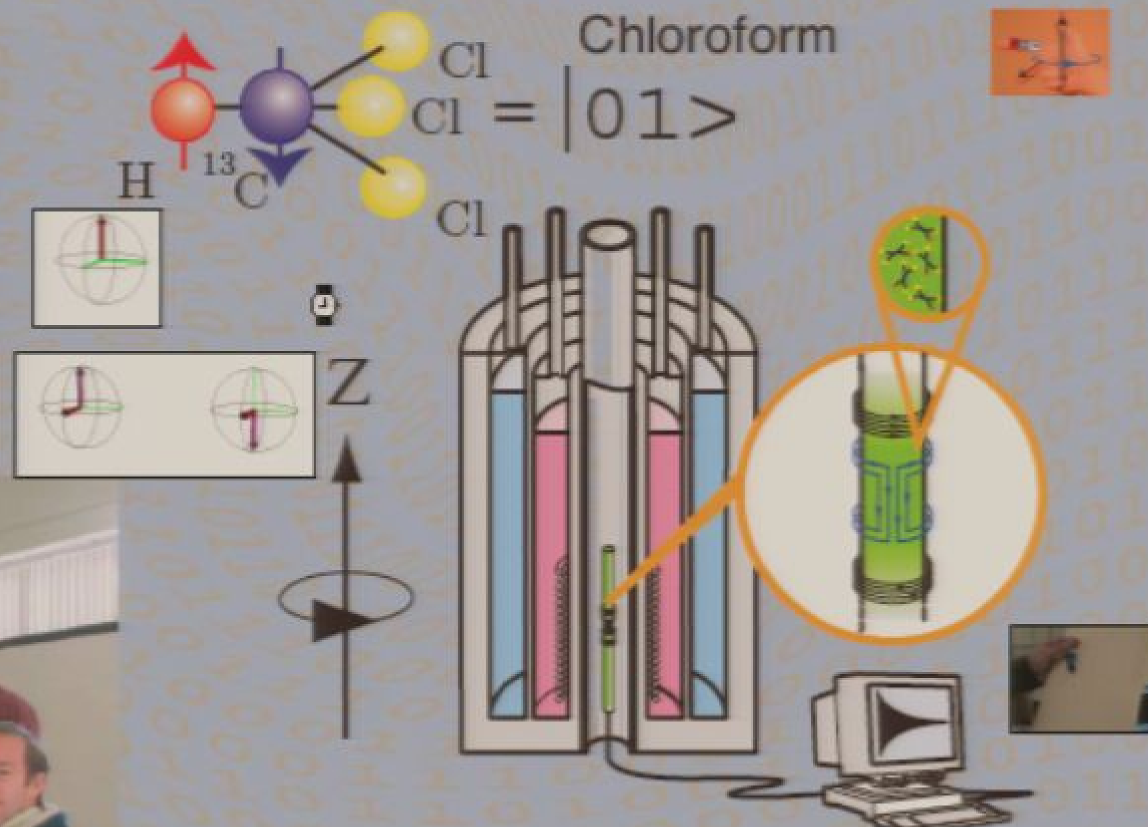
Bruker (machine) language

```
(C2_90:sp9 ph13 ):f1
 3u
 3u ipp13

 0.71365m

 8u
 8u
(C2_90:sp9 ph19):f1
 6u ipp15 ipp19
 8u
(C2_90:sp9 ph20):f1
 6u ipp15 ipp20
```

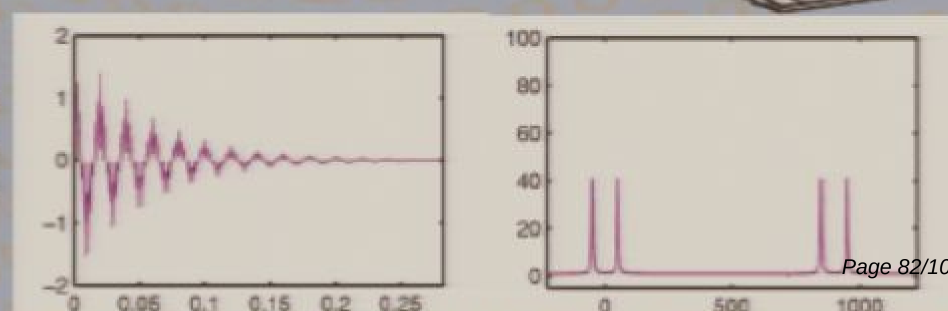
Nuclear Magnetic Resonance

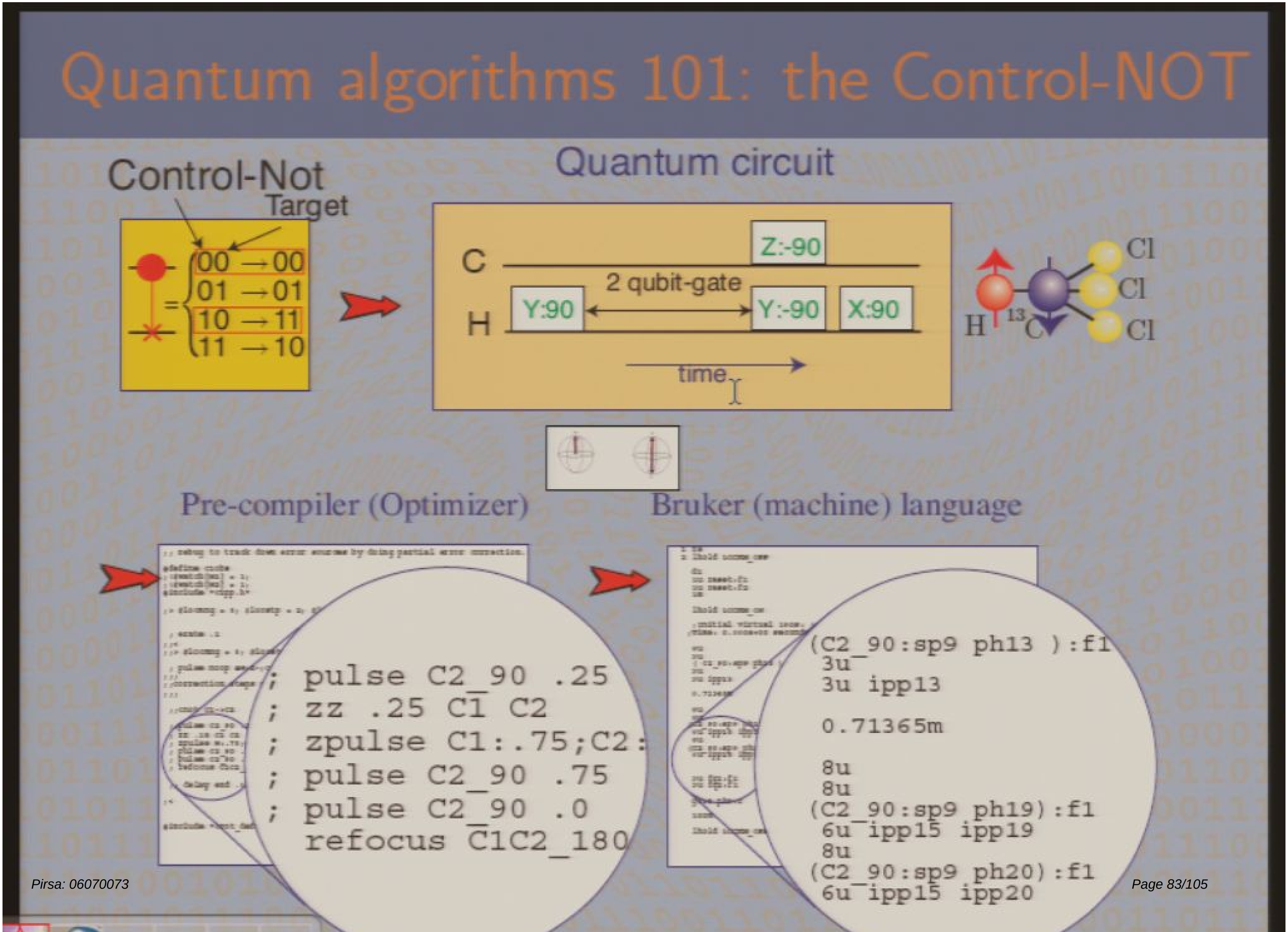
Bloch

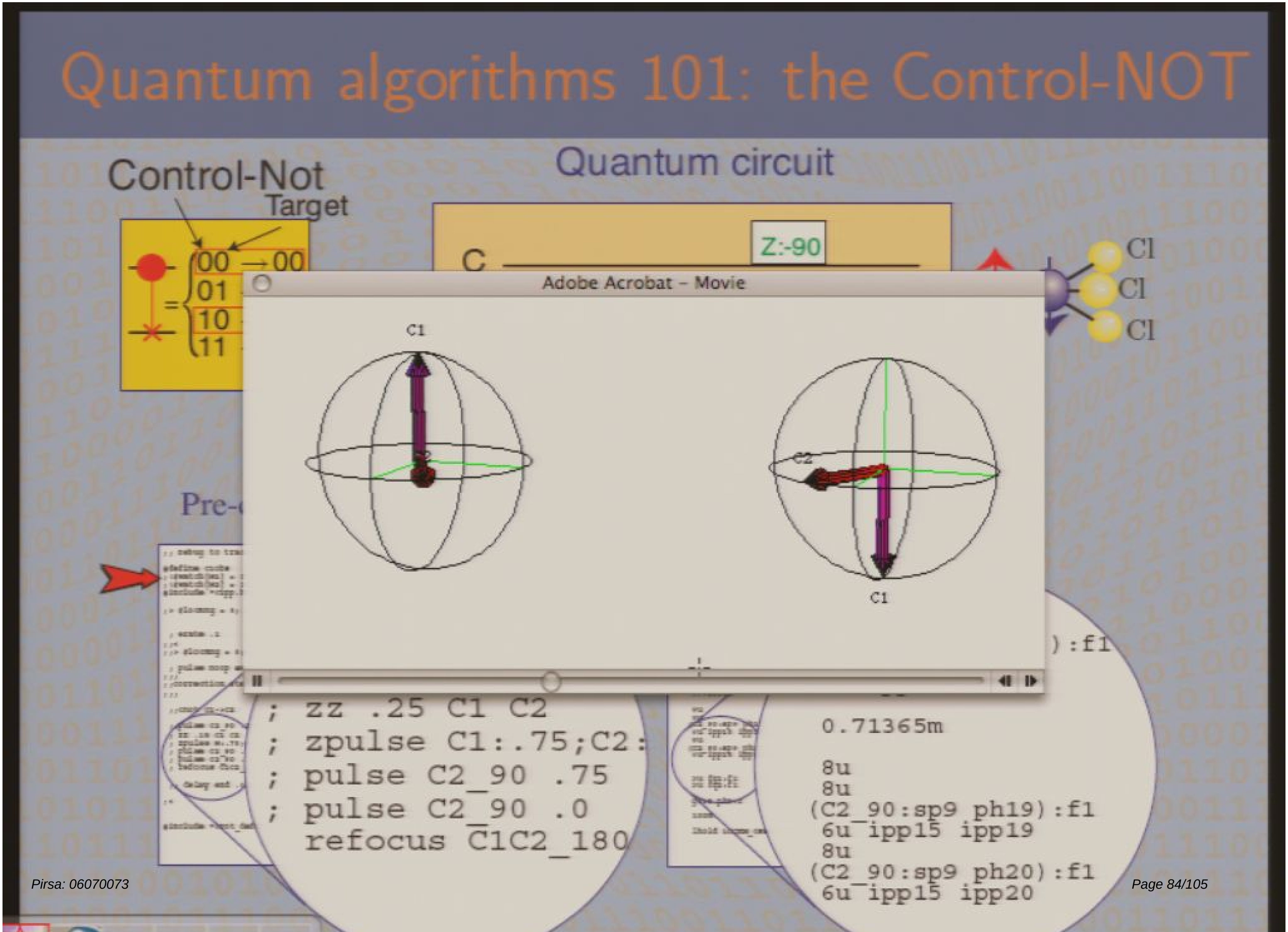
Purcell

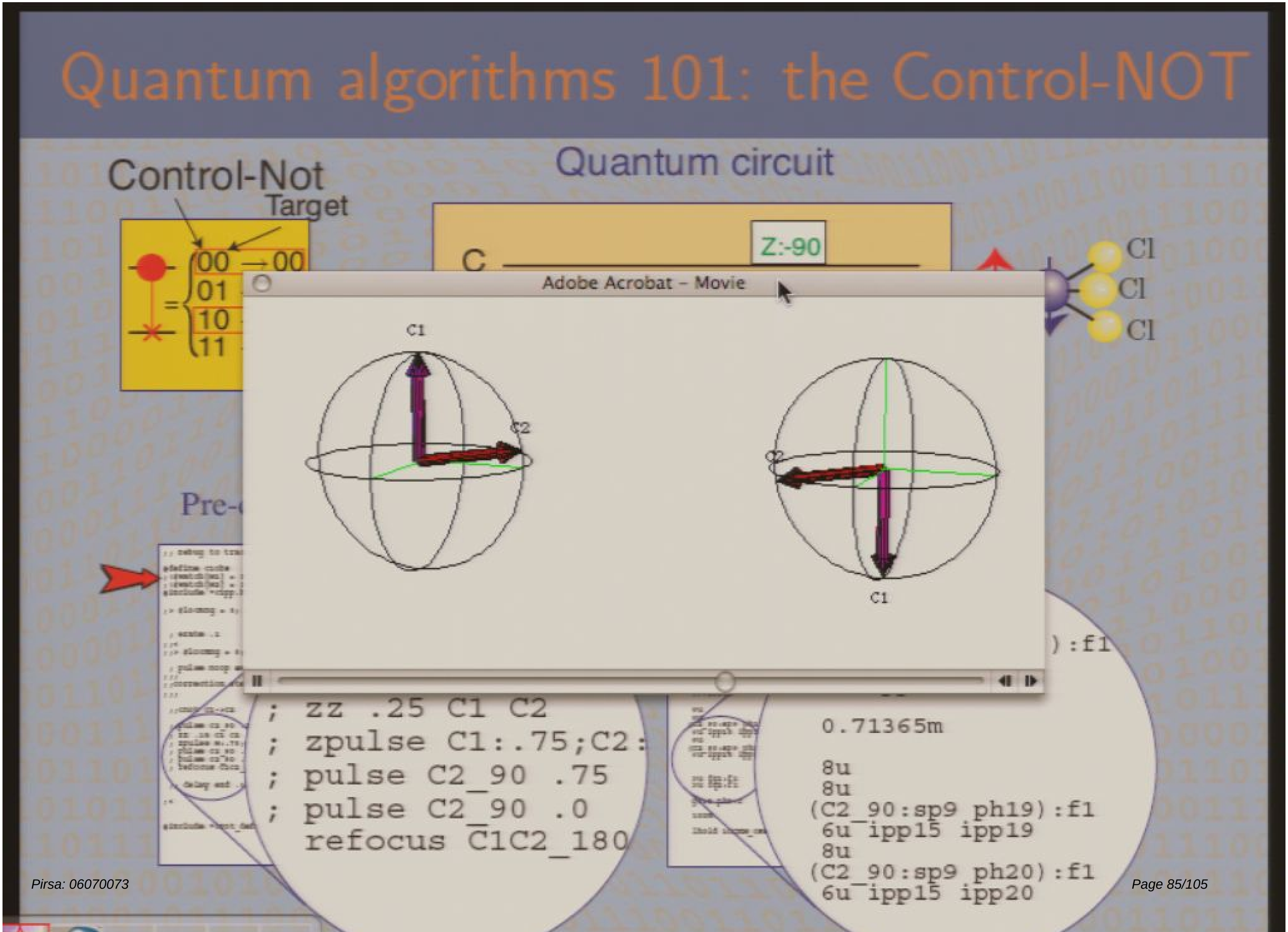


Bruker 700

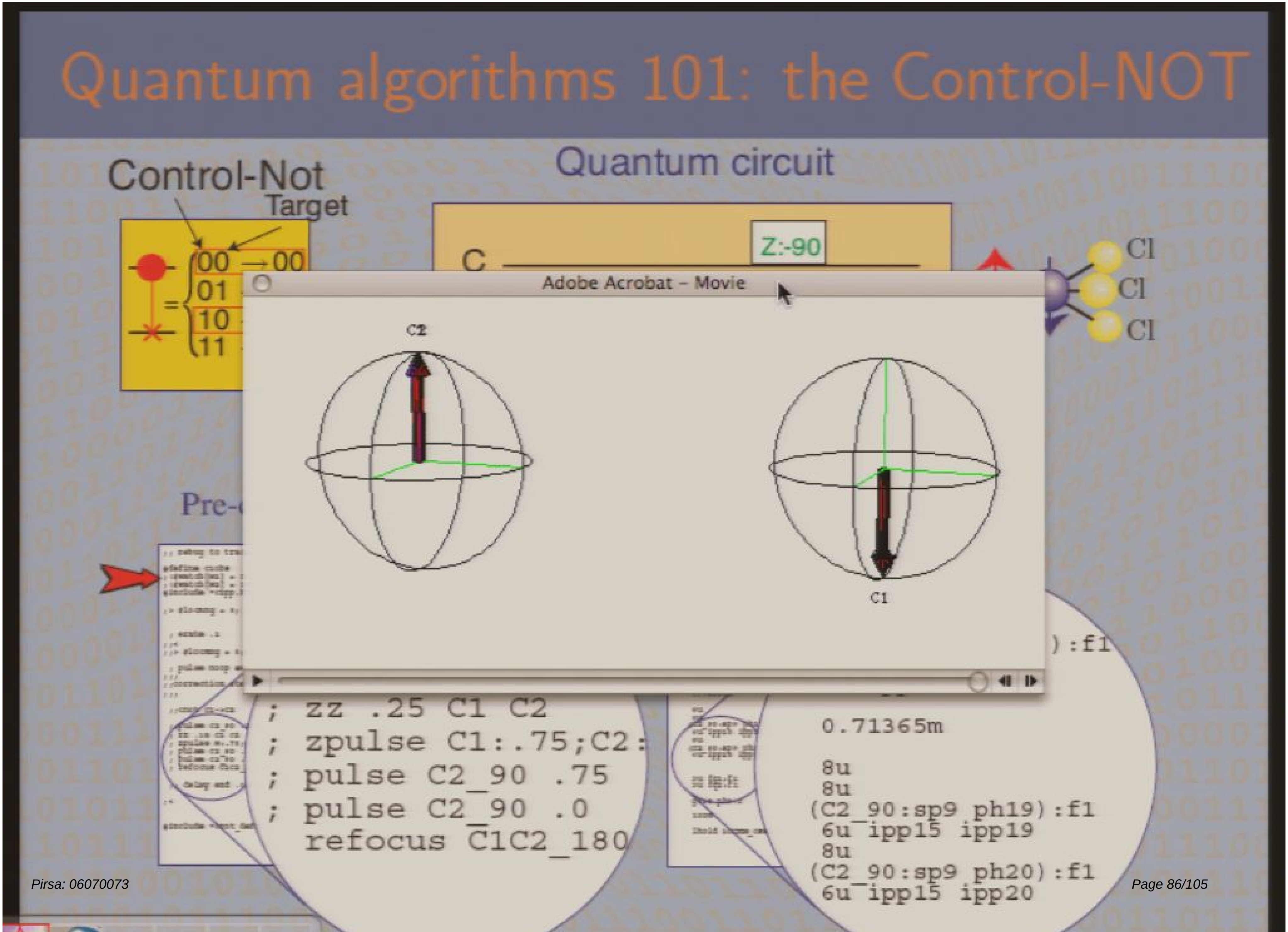


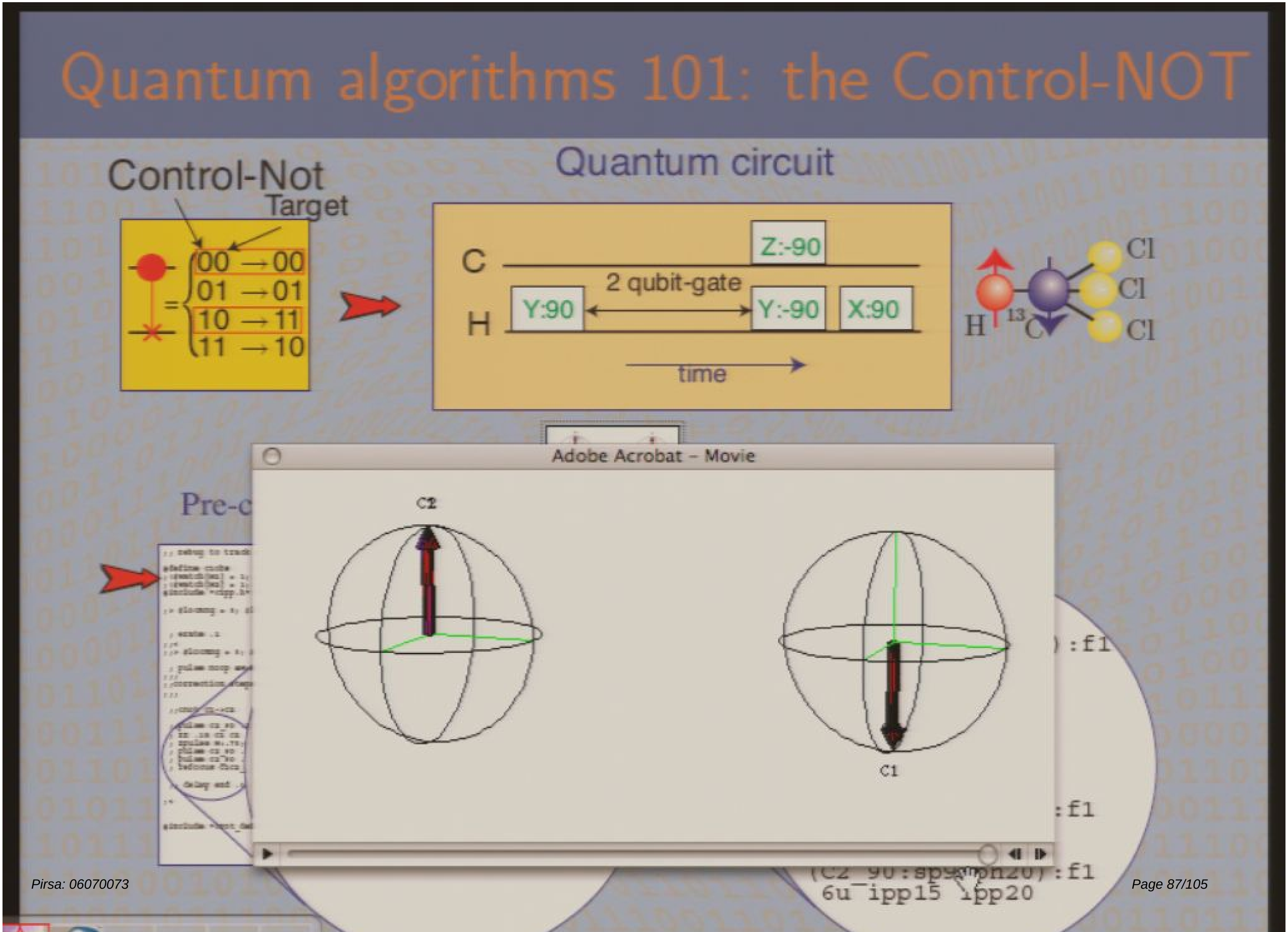

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Pre-compiler (Optimizer)
Bruker (machine) language
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
(C2_90:sp9 ph13):f1
3u
3u ipp13
0.71365m
8u
8u
(C2_90:sp9 ph19):f1
6u ipp15 ipp19
8u
(C2_90:sp9 ph20):f1
6u ipp15 ipp20


Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01
10
11
Quantum circuit
Z:-90
C
Adobe Acrobat – Movie
C1
C2
C1
Cl
Cl
Cl
Pre-
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
):f1
0.71365m
8u
8u
(C2_90:sp9 ph19):f1
6u ipp15 ipp19
8u
(C2_90:sp9 ph20):f1
6u ipp15 ipp20

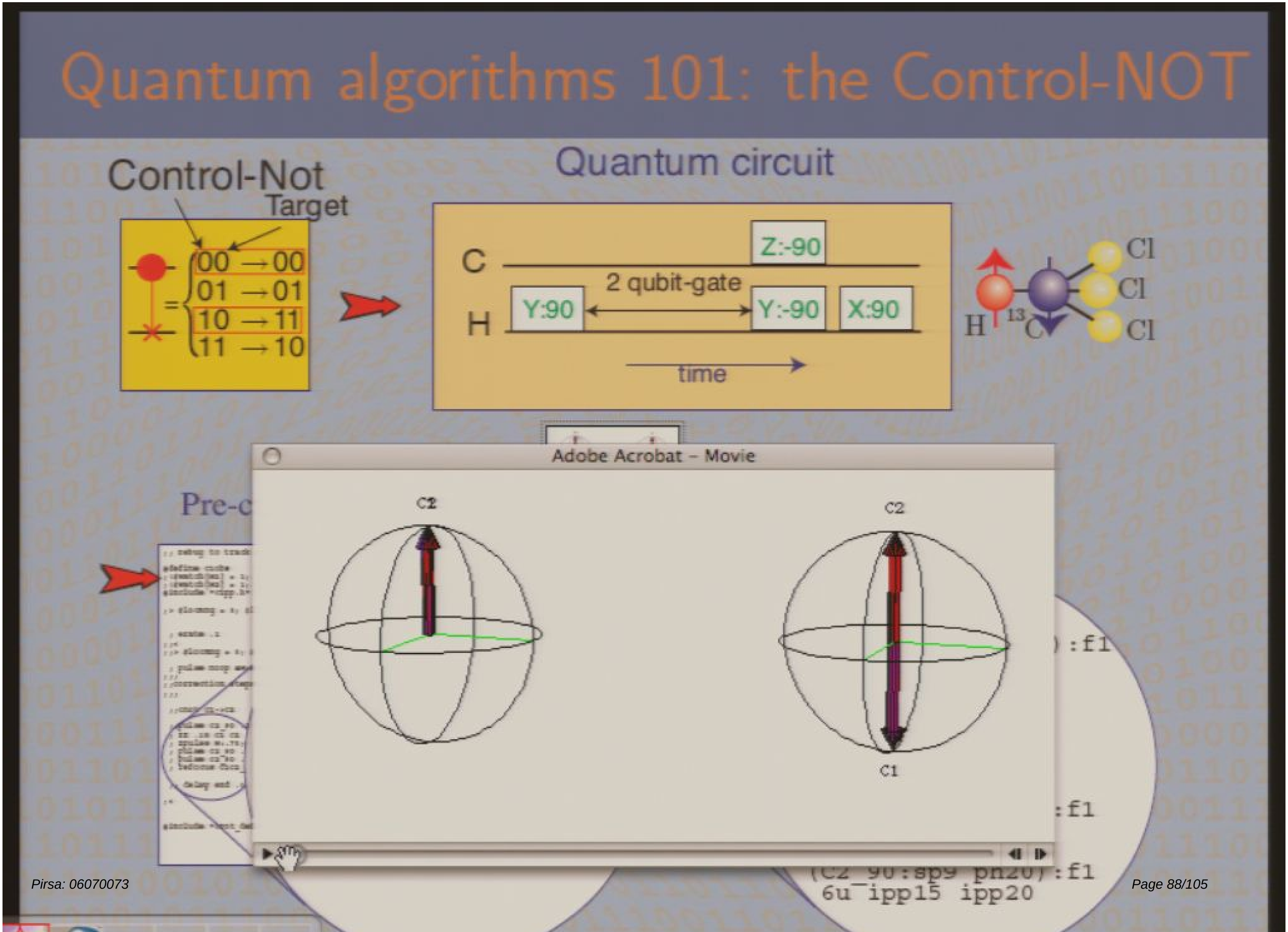


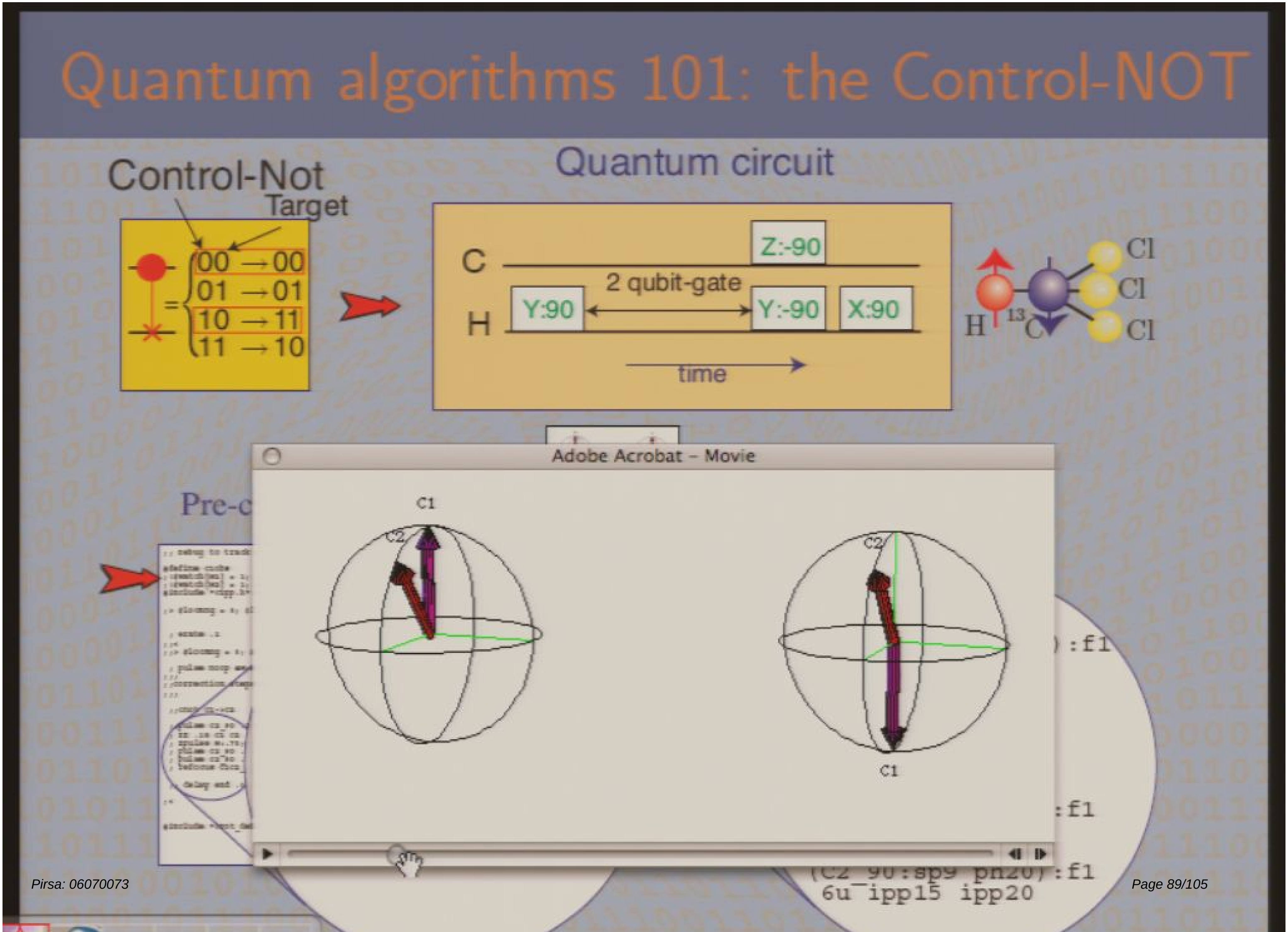
Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01
10
11
Quantum circuit
C
Z:-90
Adobe Acrobat – Movie
C1
C2
C2
C1
Cl
Cl
Cl
Pre-
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
):f1
0.71365m
8u
8u
(C2_90:sp9 ph19):f1
6u ipp15 ipp19
8u
(C2_90:sp9 ph20):f1
6u ipp15 ipp20

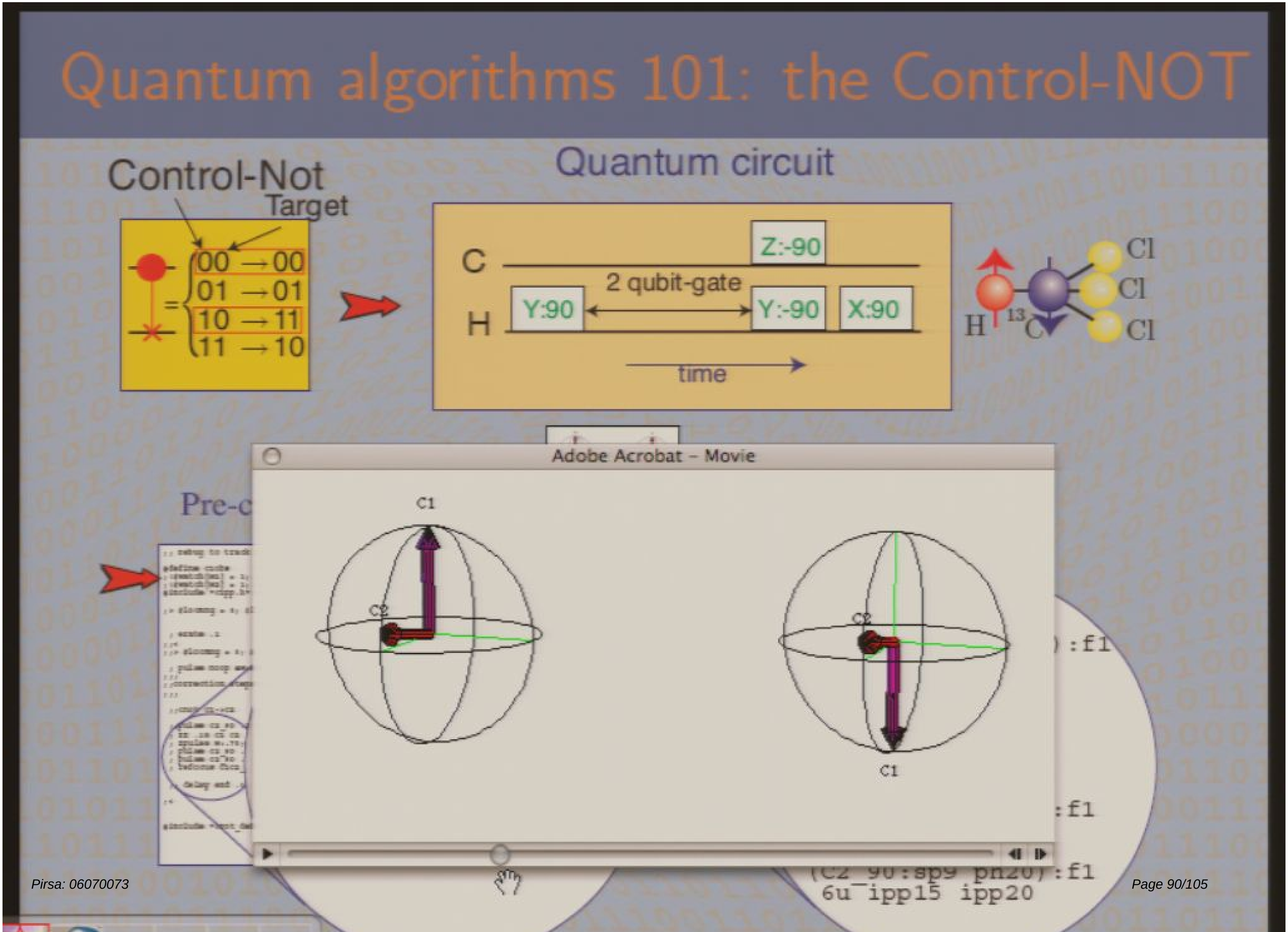

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01
10
11
Quantum circuit
Z:-90
C
Adobe Acrobat – Movie
C2
C1
Cl
Cl
Cl
Pre-
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
):f1
0.71365m
8u
8u
(C2_90:sp9 ph19):f1
6u ipp15 ipp19
8u
(C2_90:sp9 ph20):f1
6u ipp15 ipp20



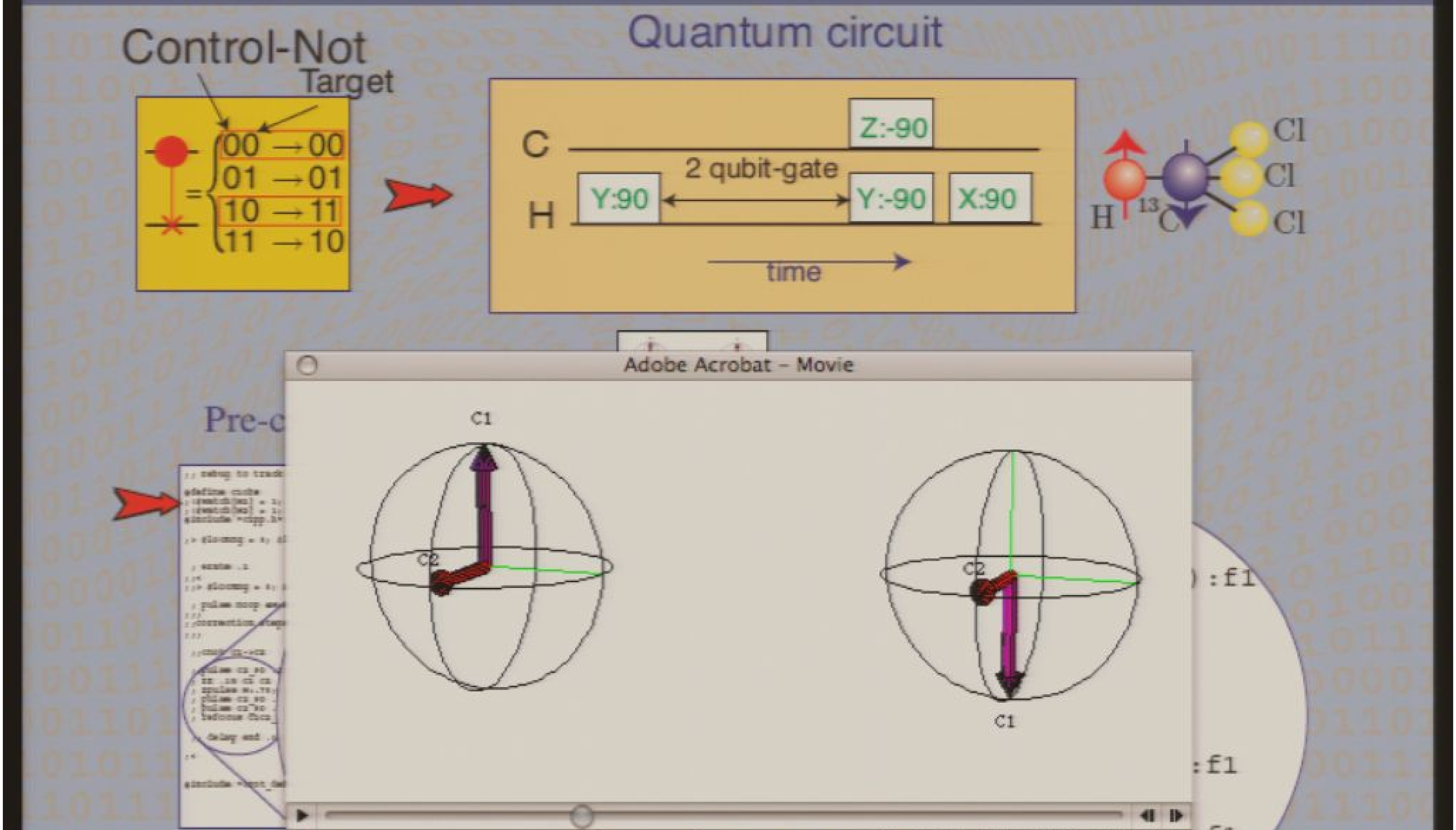
Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Adobe Acrobat – Movie
C2
C1


Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Adobe Acrobat – Movie
C2
C2
C1
Pre-c
:f1
:f1
(C2_90:sp9 ph20):f1
6u ipp15 ipp20

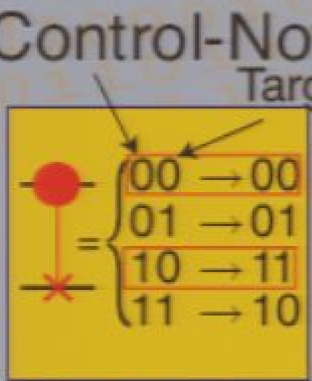

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Adobe Acrobat – Movie
C1
C2
C2
C1
):f1
:f1
(C2_90:sp9 ph20):f1
6u ipp15 ipp20


Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
Cl
Cl
Cl
H
13C
Pre-c
Adobe Acrobat – Movie
C1
C2
C2
C1
):f1
:f1
(C2 90:sp9 ph20):f1
6u ipp15 ipp20

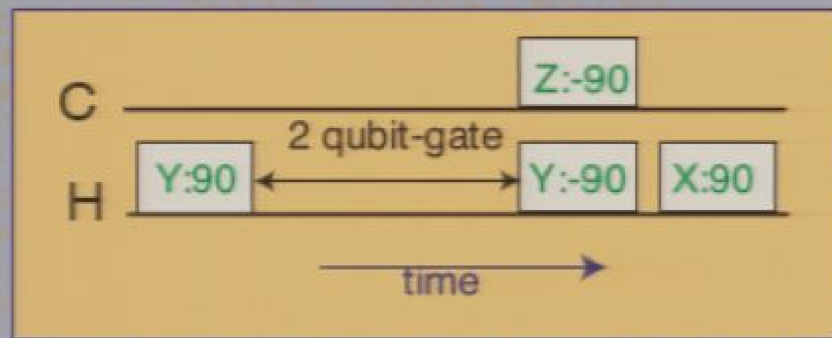
Quantum algorithms 101: the Control-NOT

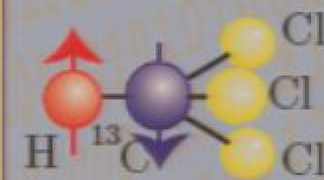


Quantum algorithms 101: the Control-NOT

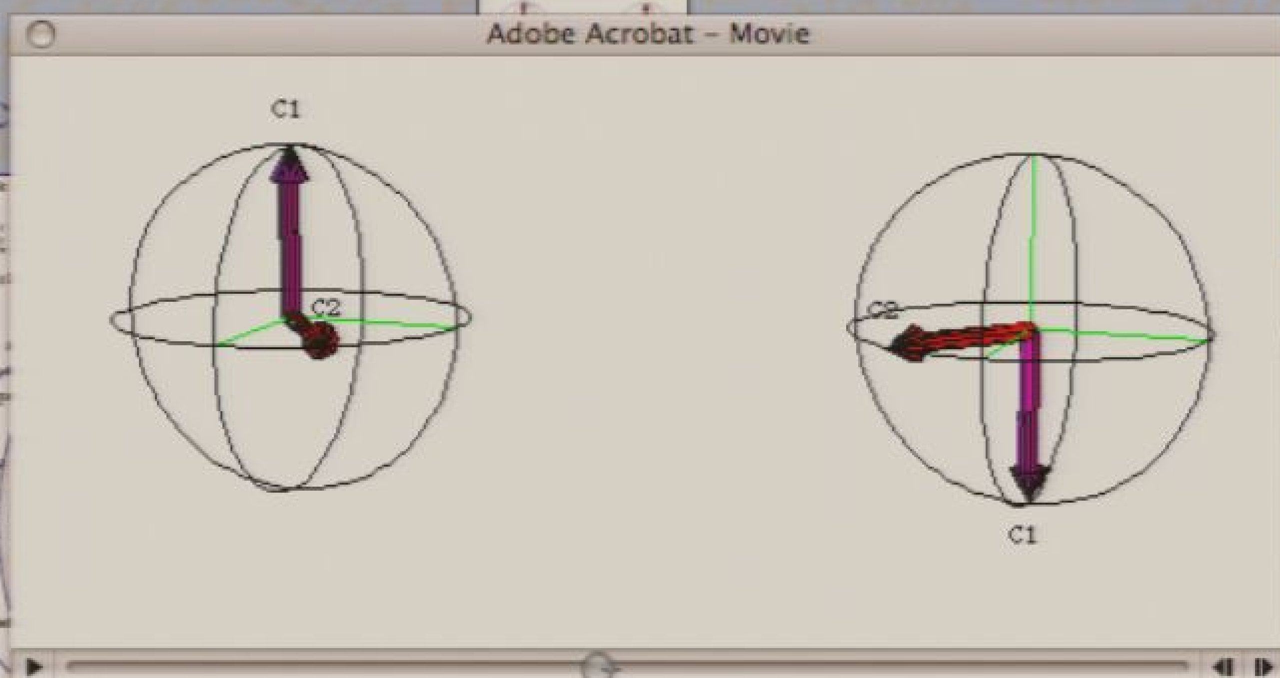


Quantum circuit





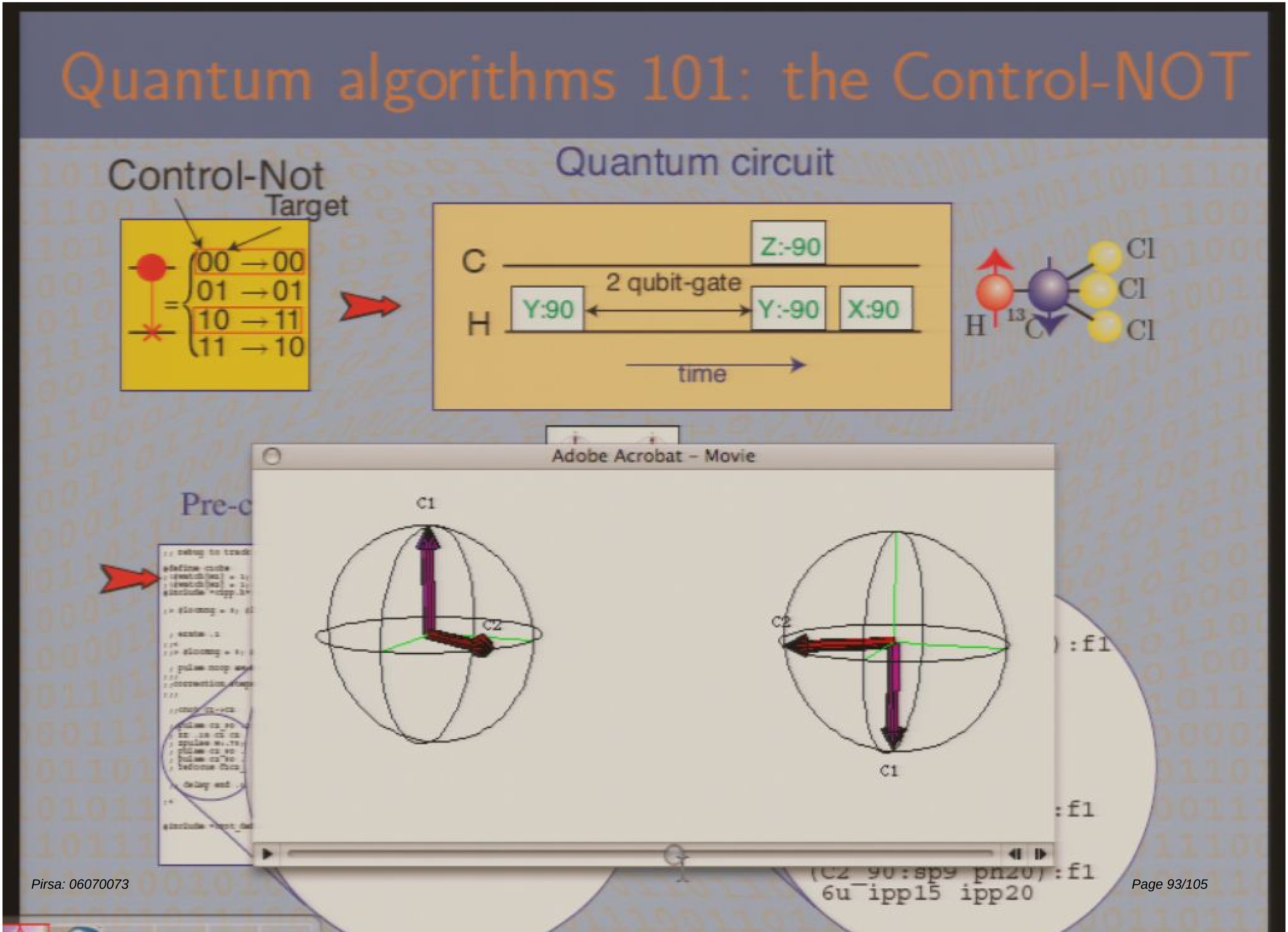
Pre-c



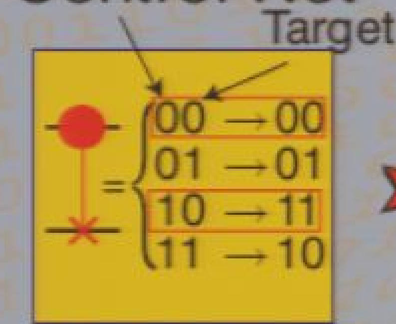
):f1

:f1

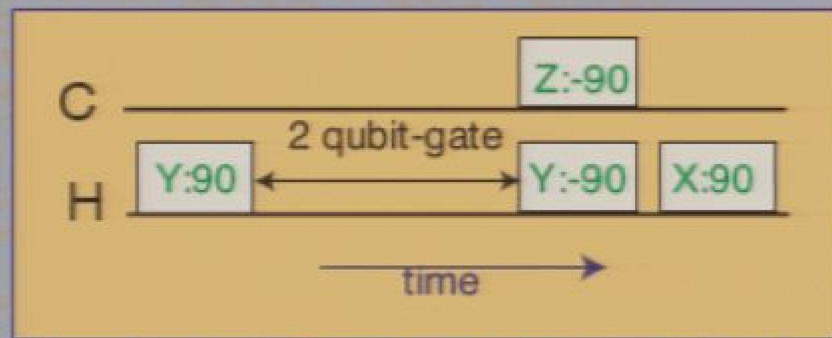
(C2_90:sp9 ph20):f1
6u ipp15 ipp20

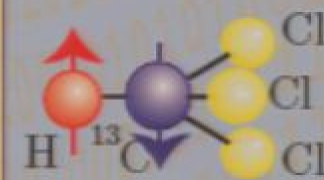

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Pre-c
Adobe Acrobat – Movie
C1
C2
C2
C1
):f1
:f1
(C2 90:sp9 ph20):f1
6u ipp15 ipp20

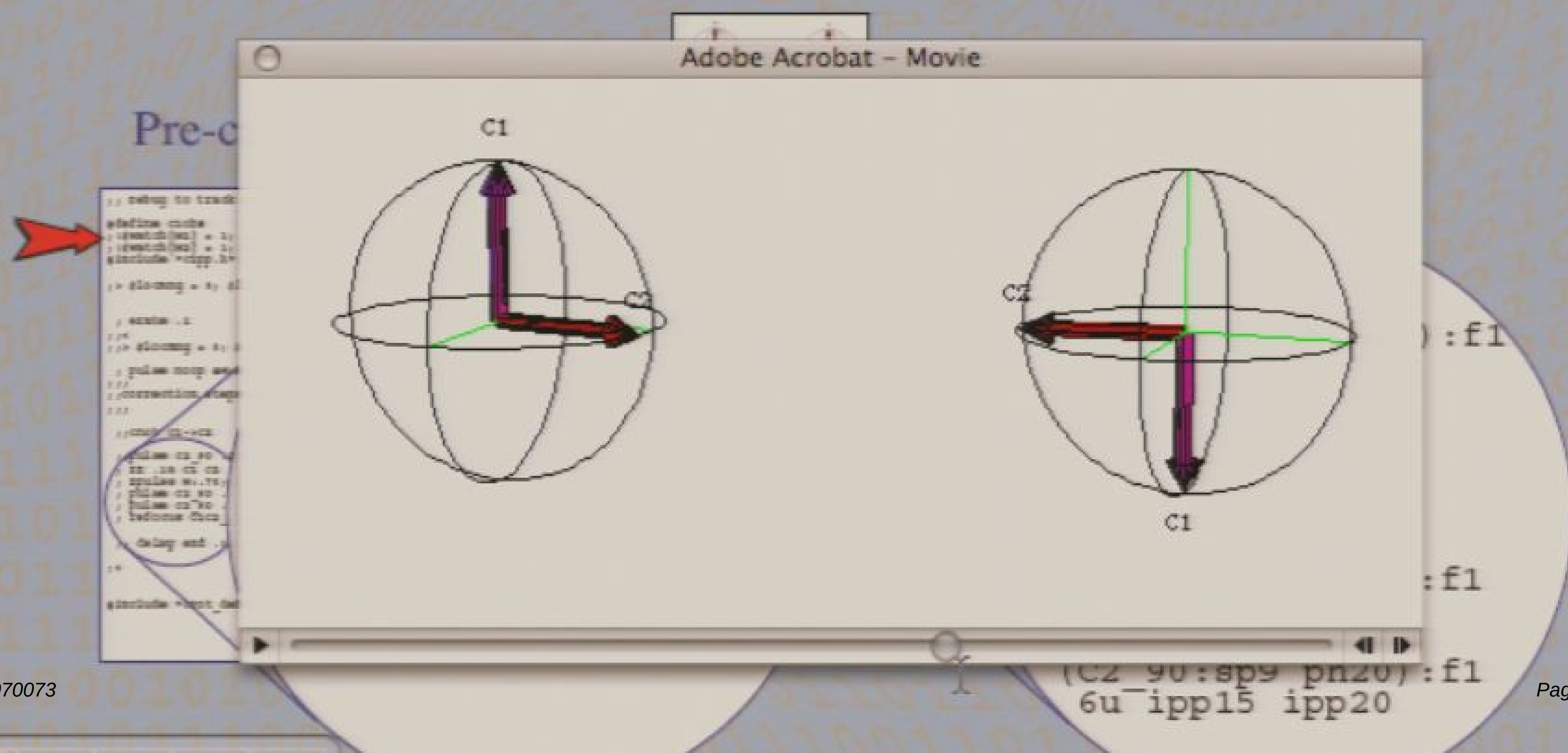
Quantum algorithms 101: the Control-NOT

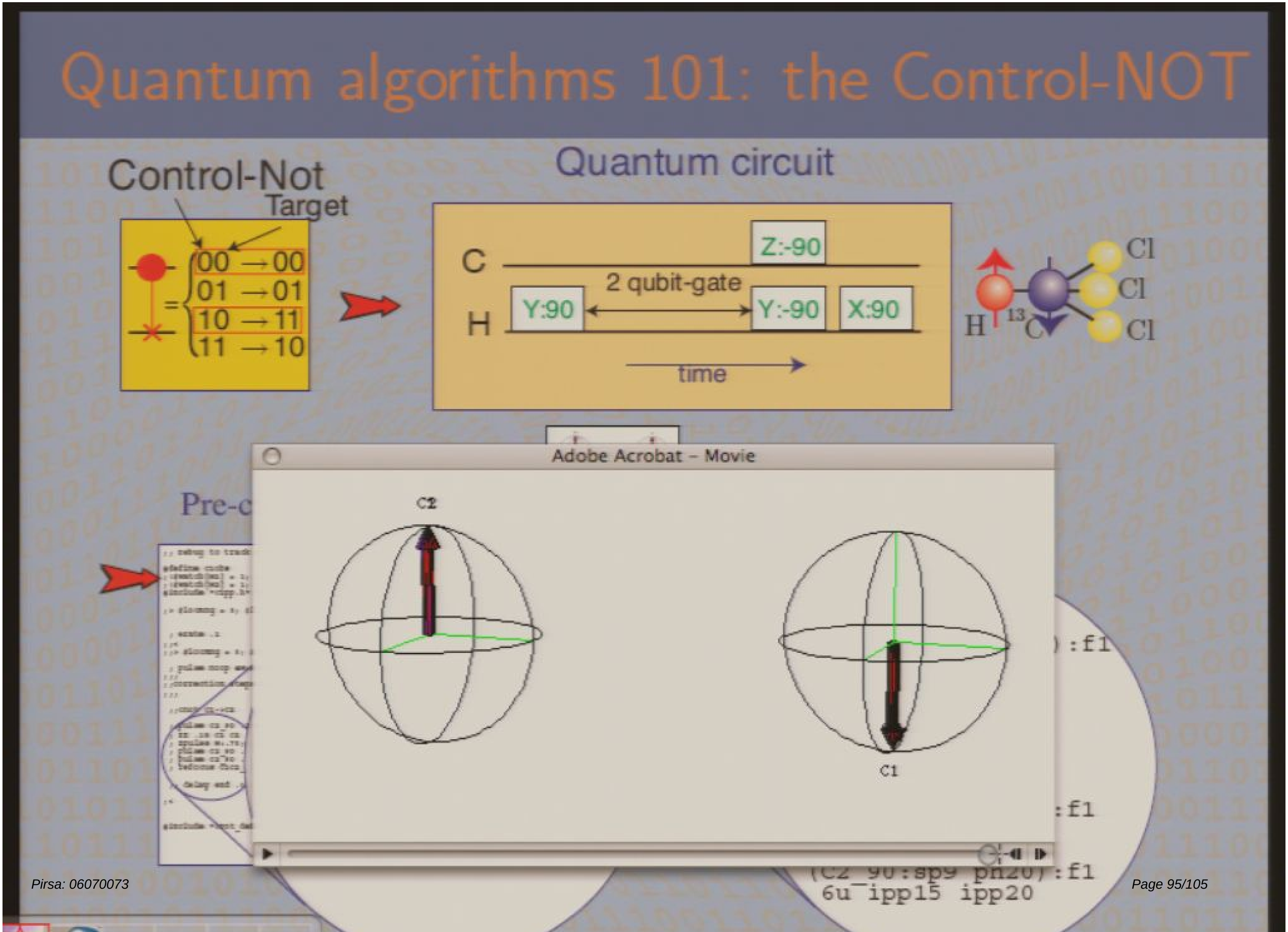


Quantum circuit



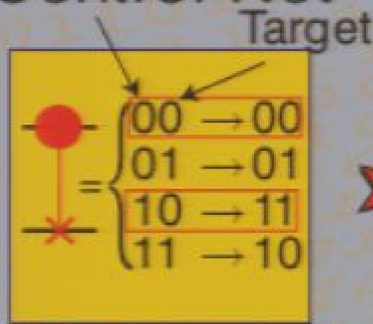




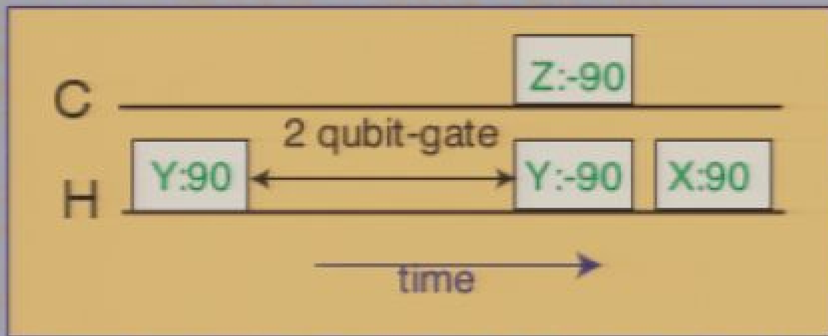

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
time
H
13C
Cl
Cl
Cl
Pre-c
Adobe Acrobat – Movie
C2
C1
):f1
:f1
(C2 90:sp9 ph20):f1
6u ipp15 ipp20

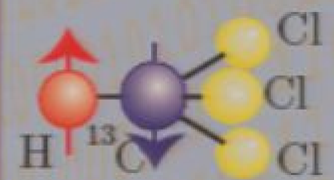
Quantum algorithms 101: the Control-NOT

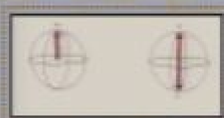
Control-Not



Quantum circuit







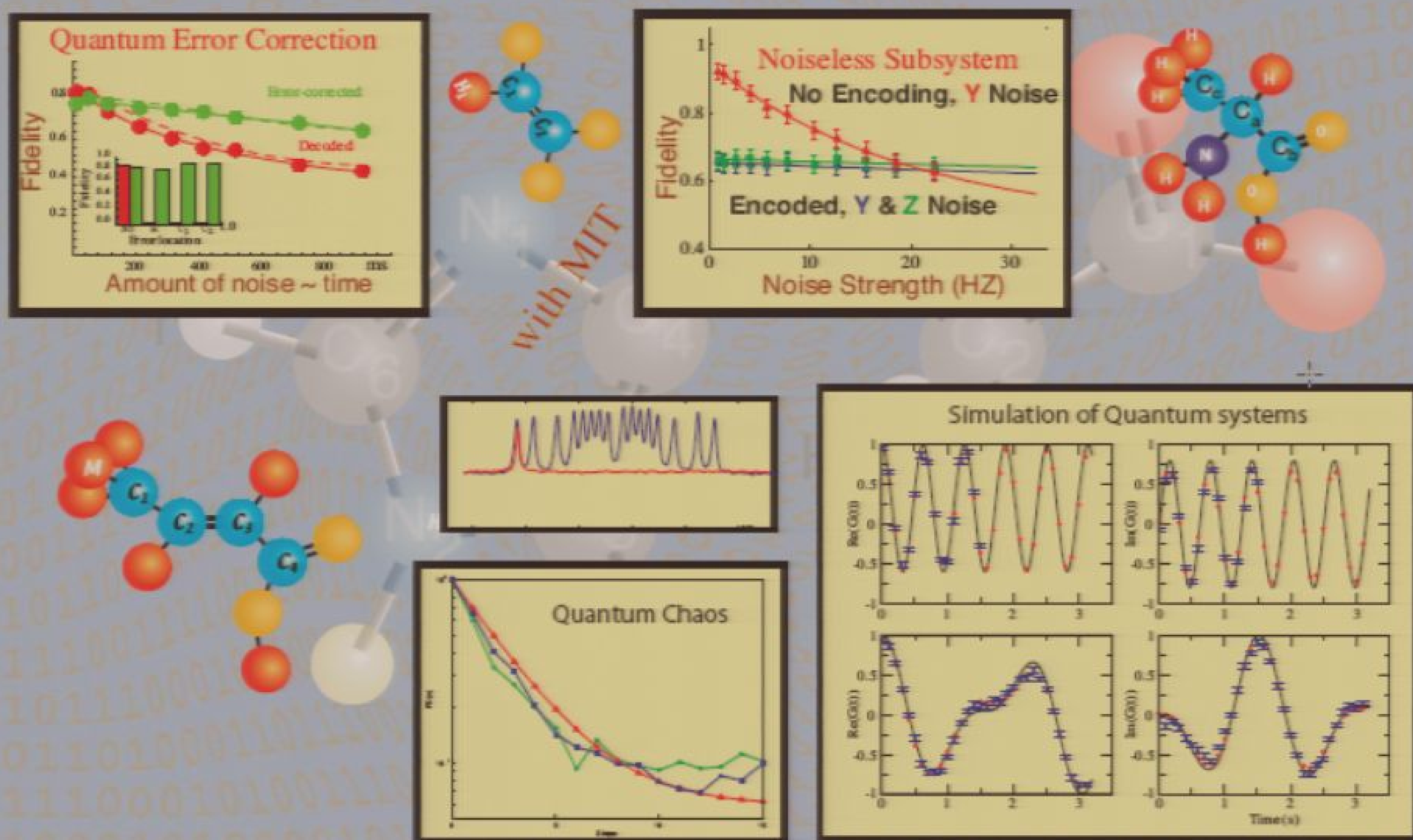
Pre-compiler (Optimizer)

```
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
  refocus C1C2_180
```

Bruker (machine) language

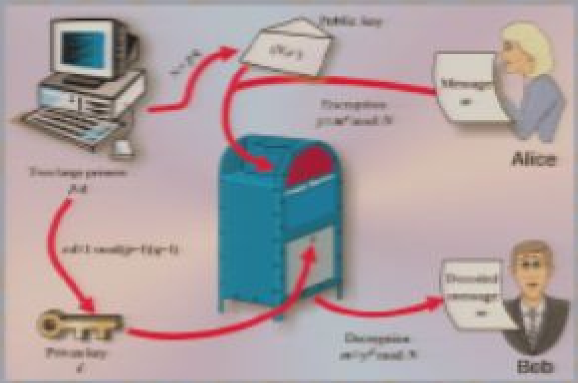
```
(C2_90:sp9 ph13 ):f1
 3u
 3u ipp13

 0.71365m

 8u
 8u
(C2_90:sp9 ph19):f1
 6u ipp15 ipp19
 8u
(C2_90:sp9 ph20):f1
 6u ipp15 ipp20
```

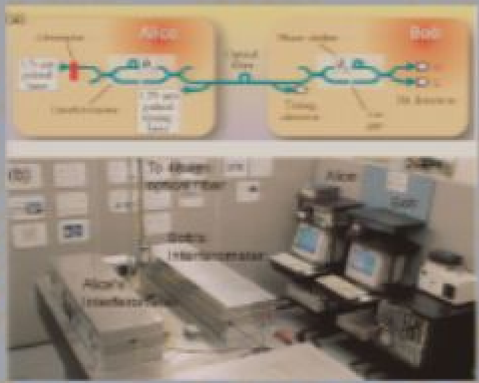
Expt. on small QIP:



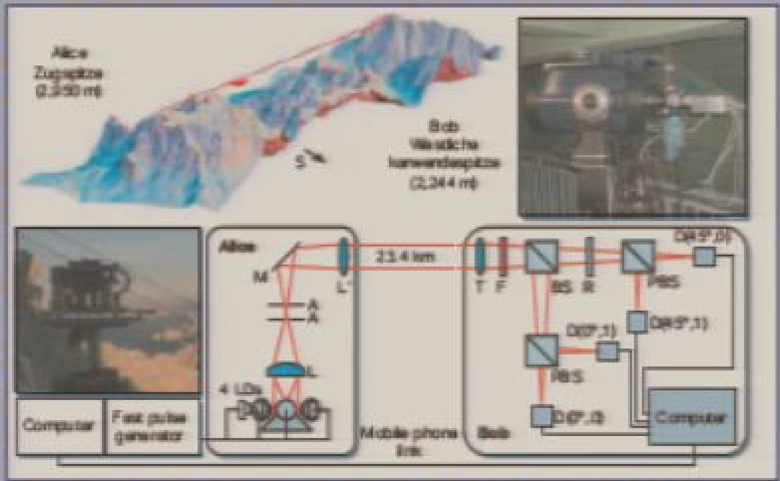
Quantum cryptography

Idea: using the inevitable disturbance in the measurement process of quantum mechanical systems as a tool to monitor eavesdropping:

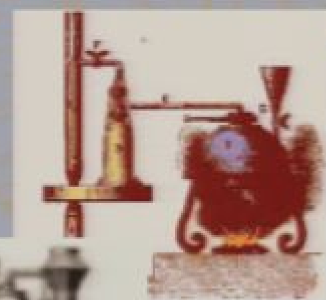


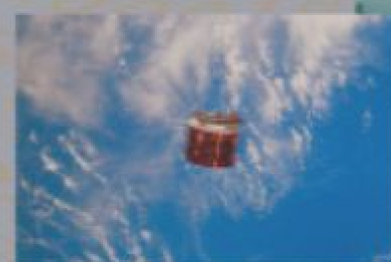


Quantum Cryptography in the world:
NSA and Los Alamos National Laboratory
www.losalamos.gov
Rarity's group
www.dera.gov.uk
The Norwegian group www.vad1.com/qcr
BBN Technologies:
www.bbn.com/networking/quantumcryptography.html
IDQuantique:
www.idquantique.com/
MagiQ:
www.magiqtech.com



Controlling forces of nature:





Conclusion

- Many of today's technologies are going towards the quantum scale.
- Quantum information take this decrease as an advantage instead of an impediment, it allows to tackle tasks impossible for its classical counterpart.

- Quantum information is the most developed of the potential quantum technologies but other ones will also be created.

Sponsors of IQC

Institute for Quantum Computing

University of Waterloo

The National Security Agency

ARDA

NSERC CRSNG

SJU

Ontario Innovation Trust

mitacs

ONTARIO CHALLENGE FUND

Putting R&D to Work

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

Canada Research Chairs — Chaires de recherche du Canada

Communications Security Establishment — Centre de la sécurité des télécommunications

Premier's Research Excellence Awards

sgi

BRUKER canada

helios | oceana

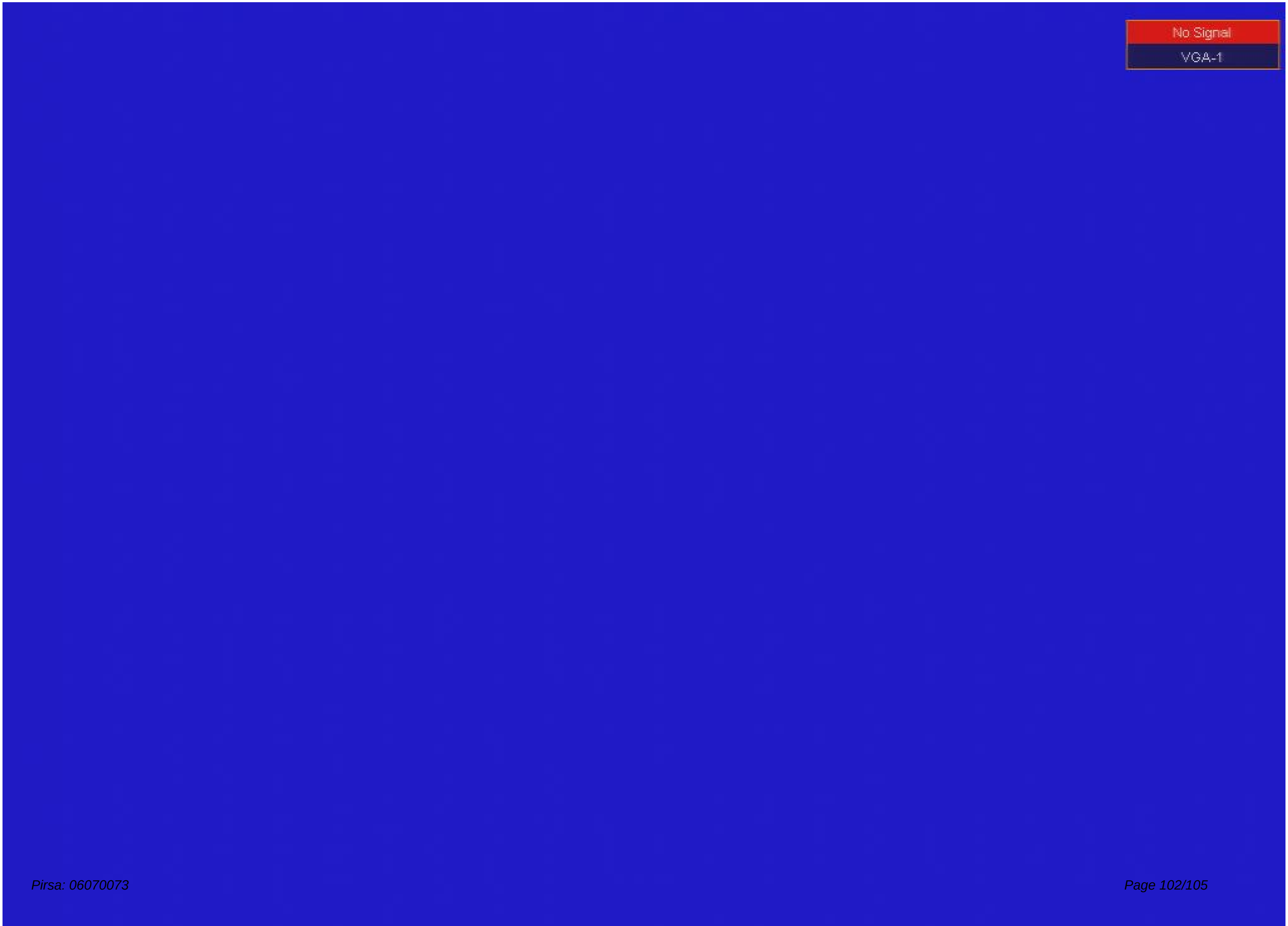
Sun microsystems

PI

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

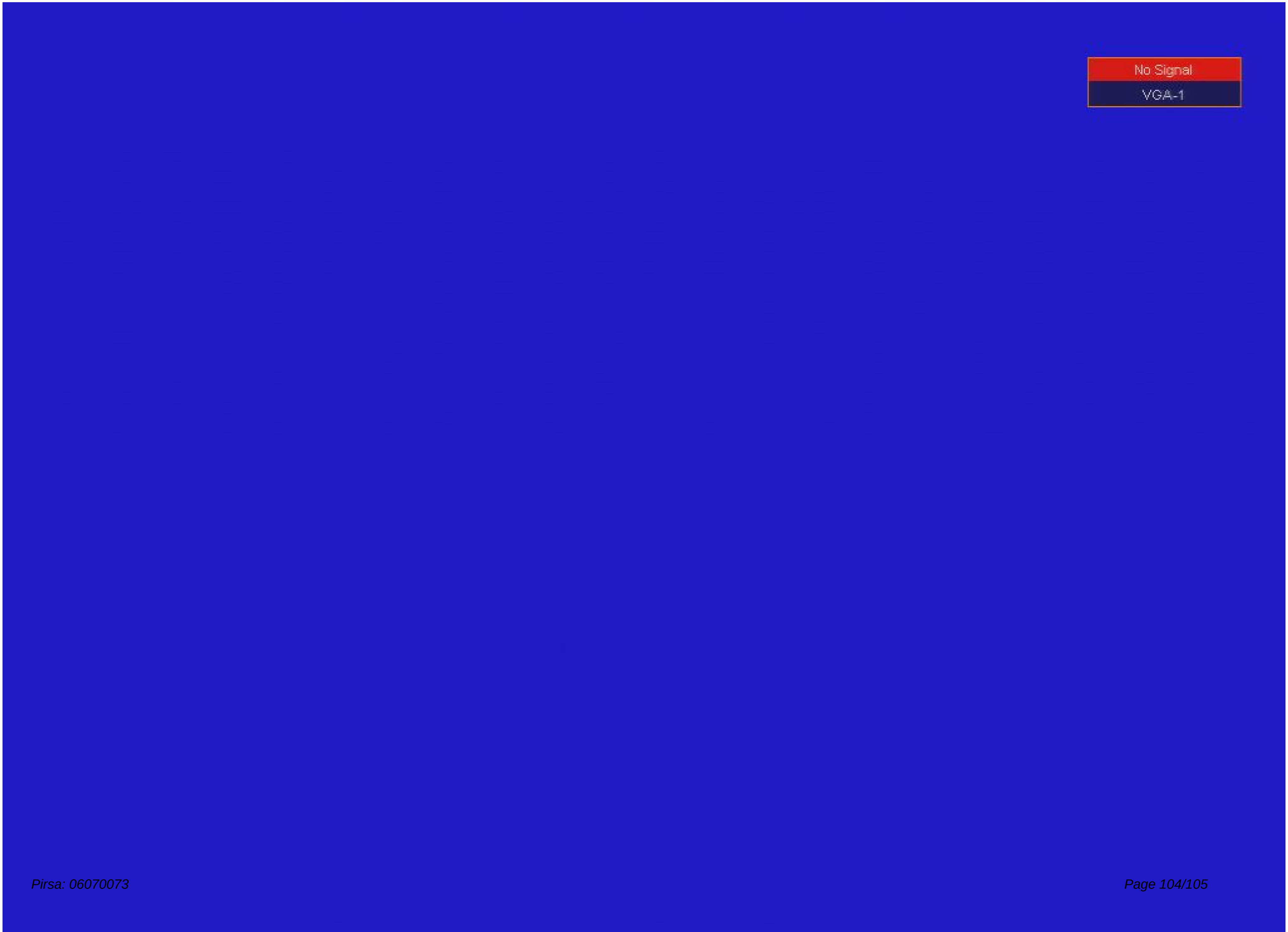
Centre for Applied Cryptographic Research

The University of Waterloo


No Signal
VGA-1

No Signal

VGA-1


No Signal
VGA-1

PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS