Title: Harnessing the Quantum World

Date: Dec 02, 2004 04:20 PM

URL: http://pirsa.org/04120002

Abstract: Are you ready for this upgrade? The very foundation of computer science is changing. As Moore\'s Law draws to a close, rules of quantum physics are taking over. Learn how leading researchers are using counterintuitive effects, such as superposition, in their quest to build ultra-powerful quantum computers. You\'ll see how quantum particles behave, are controlled and, ultimately, used to calculate. <kw>quantum world, Raymond Laflamme, quantum mechanics, quantum information, quantum computing, information processing, Moore\'s Law, quantum scale, complexity theory, cryptography, qubits, quantum bits, quantum states, nuclear magnetic resonance, Turing </kw>

Harnessing the Quantum World

IQC Institute *for* Quantum Computing

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Harnessing the Quantum World

IQC
Institute for Quantum Computing
University of Waterloo

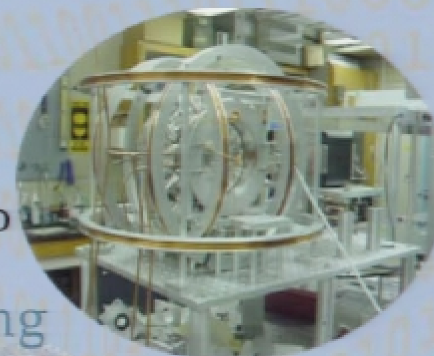
Raymond Laflamme
laflamme@iqc.ca

Harnessing the Quantum World

Harnessing the Quantum World

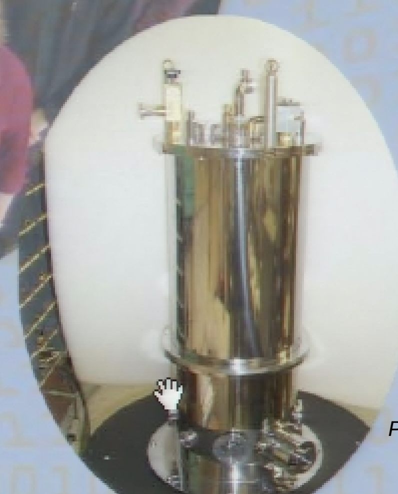
IQC

University of Waterloo



Institute *for* Quantum Computing

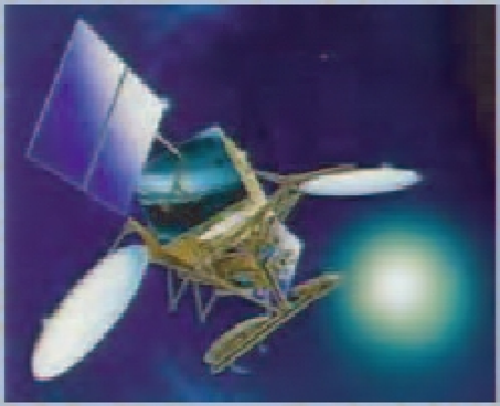
Raymond Laflamme
laflamme@iqc.ca



Plan

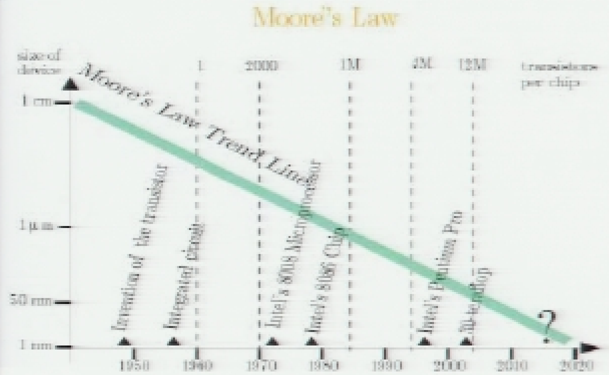
- Why quantum information?
- What is quantum computing?
- Steps towards building these devices.

Information Processing Devices



Why Quant. Info. Processing?

We are advancing towards the quantum scale!



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

www.sciencemag.org SCIENCE VOL 285 24 SEPTEMBER 1999

SCIENCE'S COMPASS

PERSPECTIVES: DEVICE PHYSICS

Pushing the Limits

Paul A. Packan

For the past 30 years, the semiconductor industry has followed Moore's law, which states that transistor performance and density double every 3 years (*1*). Although not truly a law, Gordon Moore's statement has yet to be violated. But now it seems to be in serious danger. Fundamental thermodynamic limits are being reached in critical areas, and unless new, innovative solutions are found, the current rate of improvement cannot be maintained.

The dominant electronic device used today in integrated circuits is the silicon-

silicor is cov neighl atom the m ing ar with c accept con at tra ele free cl tor sca... centration of these donor and accepto atoms to maintain a constant total charg

These fundamental issues have not previously limited the scaling of transistors and represent a considerable challenge for the semiconductor industry. There are currently no known solutions to these problems. To continue the performance trends of the past 20 years and maintain Moore's law of improvement will be the most difficult challenge the semiconductor industry has ever faced.

References

1. G. Moore, *IEDM Tech. Dig.* (1975), p. 11.
2. R. H. Dennard et al., *IEEE J. Solid-State Circuits* SC-9,

The author is at Intel Corporation, 5200 NE Elam Parkway, Hillsboro, OR 97124, USA. E-mail: paul.a.packan@intel.com

Enterprise hardware

Intel scientists find wall for Moore's Law

Last modified: December 1, 2003, 4:00 AM PST

By Michael Kanellos
Staff Writer, CNET News.com

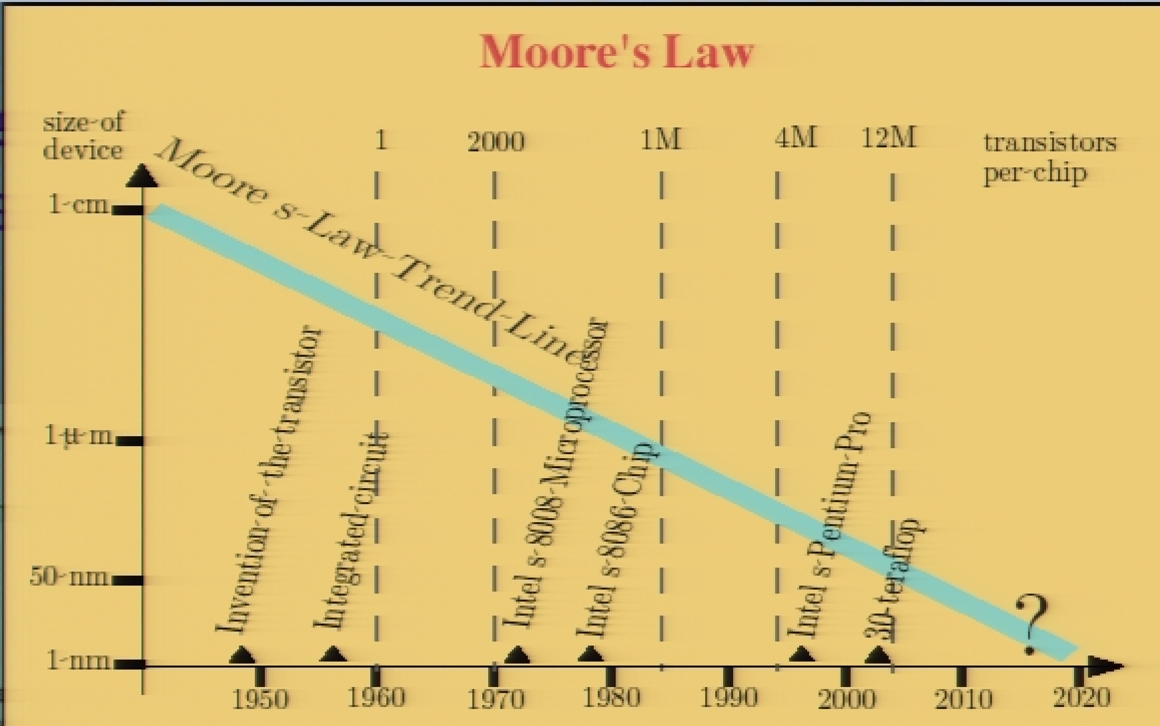
Moore's Law, as chip manufacturers generally refer to it today, is coming to an end, according to a recent research paper.

Granted, that end likely won't come for about two decades, but Intel researchers have recently published a paper theorizing that chipmakers will hit a wall when it comes to shrinking the size of transistors, one of the chief methods for making chips that are smaller, more powerful and cheaper than their predecessors.

Manufacturers will be able to produce chips on the 16-nanometer manufacturing process, expected by conservative estimates to arrive in 2018, and maybe one or two manufacturing processes after that, but that's it.

Why Quant. Info. Processing?

We are ...
the qua...



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

PERSPECT...

For the pa... tor indu... law, whi... formance and... (1). Althoug... Moore's state... But now it s... Fundamental... being reached in critical areas, and unless new, innovative solutions are found, the current rate of improvement cannot be maintained.

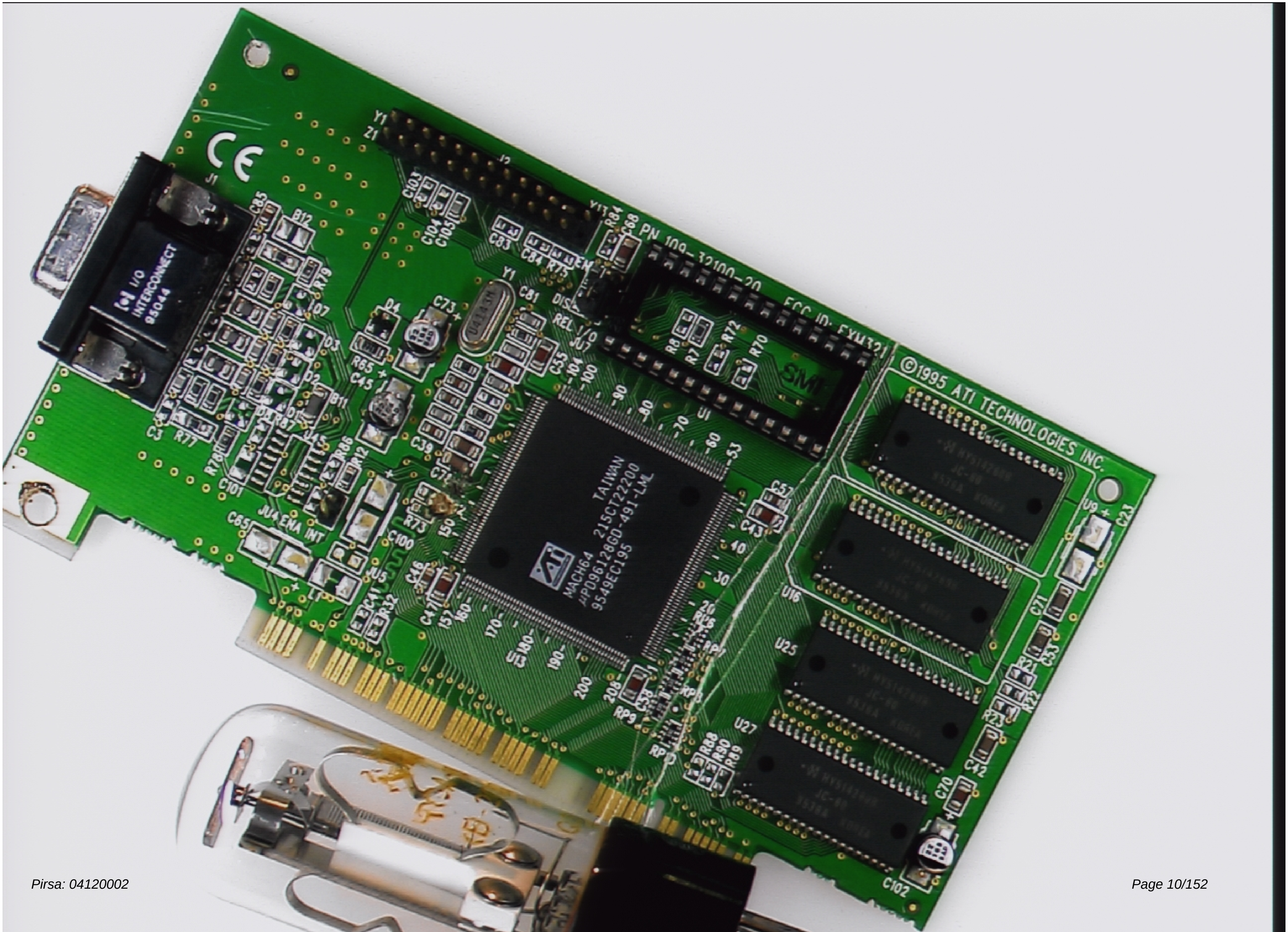
The dominant electronic device used today in integrated circuits is the silicon-

...find wall for Moore's Law

...manufacturers generally refer to it today, ...according to a recent research paper.

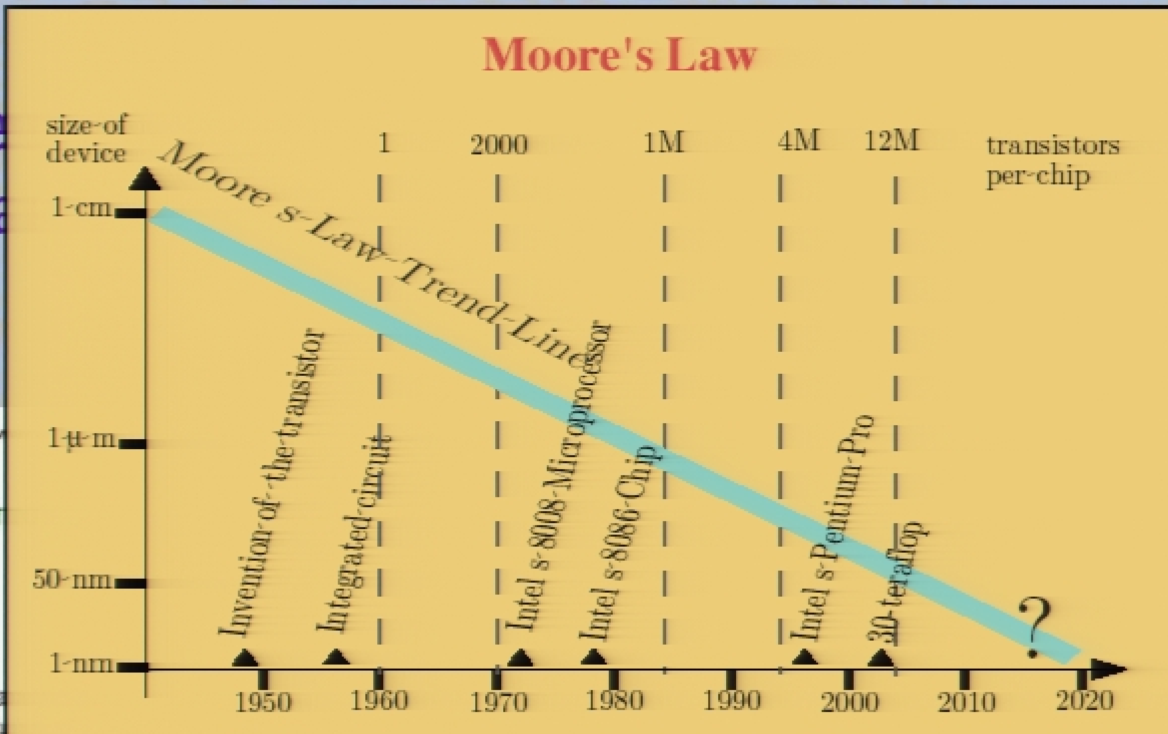
References
1. G. Moore, *IEDM Tech. Dig.* (1975), p. 11.

The author is at Intel Corporation, 5200 NE Elam Parkway, Hillsboro, OR 97124, USA. E-mail: paul.a.packan@intel.com


©1995 ATI TECHNOLOGIES INC.
I/O INTERCONNECT 95044
TAIWAN
MACH64 215CT22200
9549EC195

Why Quant. Info. Processing?

We are … the qua…



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

PERSPECT…

For the pa… tor indu… law, whi… formance and… (1). Althoug… Moore's state… But now it se… Fundamental… being reached in critical areas, and unless new, innovative solutions are found, the current rate of improvement cannot be maintained.

The dominant electronic device used today in integrated circuits is the silicon-

con at… tra ele… free cl… tor sca… centration of these donor and accepto… atoms to maintain a constant total charg…

References
1. G. Moore, *IEDM Tech. Dig.* (1975), p. 11.
2. R. H. Dennard et al., *IEEE J. Solid-State Circuits* SC-9,

The author is at Intel Corporation, 5200 NE Elam Parkway, Hillsboro, OR 97124, USA. E-mail: paul.a.packan@intel.com

…rdware

… find wall for Moore's Law

… manufacturers generally refer to it today, … according to a recent research paper.

… won't come for about two decades, but Intel … ly published a paper theorizing that … when it comes to shrinking the size of … hief methods for making chips that are … and cheaper than their predecessors.

… manufacturers will be able to produce chips on the 16-nanometer manufacturing process, expected by conservative estimates to arrive in 2018, and maybe one or two manufacturing processes after that, but that's it.

Why Quant. Info. Processing?

Where the technology is going...

Quantum mechanics was discovered 100 years ago:

- for more than the first half a century we struggled to understand its implications at describing the world around us: quantum mechanics is seen as an obstacle
- there has been technology using some feature of quantum mechanics: the transistor, the laser, MRI
- Moore's law suggests that we need to control quantum systems
- around 1980 things have started to change...

being reached in critical areas, and unless new, innovative solutions are found, the current rate of improvement cannot be maintained.

The dominant electronic device used today in integrated circuits is the silicon-

has ever faced.

References

1. G. Moore, *IEDM Tech. Dig.* (1975), p. 11.

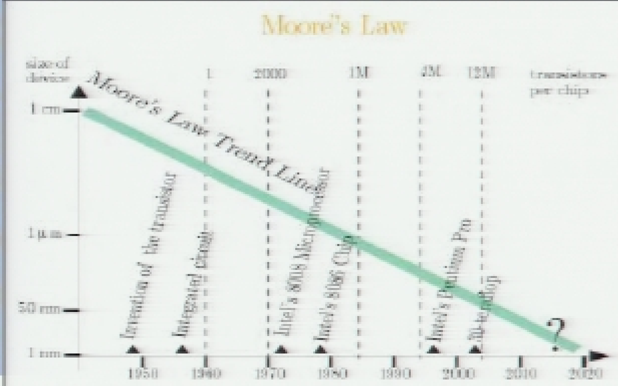
2. R. H. Dennard et al., *IEEE J. Solid-State Circuits* SC-9,

The author is at Intel Corporation, 5200 NE Elam Parkway, Hillsboro, OR 97124, USA. E-mail: paul.a.packan@intel.com

Manufacturers will be able to produce chips on the 16-nanometer manufacturing process, expected by conservative estimates to arrive in 2018, and maybe one or two manufacturing processes after that, but that's it.

Why Quant. Info. Processing?

We are advancing towards the quantum scale!



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

www.sciencemag.org SCIENCE VOL 285 24 SEPTEMBER 1999

SCIENCE'S COMPASS

PERSPECTIVES: DEVICE PHYSICS

Pushing the Limits

Paul A. Packan

For the past 30 years, the semiconductor industry has followed Moore's law, which states that transistor performance and density double every 3 years (*1*). Although not truly a law, Gordon Moore's statement has yet to be violated. But now it seems to be in serious danger. Fundamental thermodynamic limits are being reached in critical areas, and unless new, innovative solutions are found, the current rate of improvement cannot be maintained.

The dominant electronic device used today in integrated circuits is the silicon-

silicor is cov neighl atom the m ing ar with c accept con at tra ele free cl tor scaling ... centration of these donor and accepto atoms to maintain a constant total charg

These fundamental issues have not previously limited the scaling of transistors and represent a considerable challenge for the semiconductor industry. There are currently no known solutions to these problems. To continue the performance trends of the past 20 years and maintain Moore's law of improvement will be the most difficult challenge the semiconductor industry has ever faced.

References

1. G. Moore, *IEDM Tech. Dig.* (1975), p. 11.
2. R. H. Dennard et al., *IEEE J. Solid-State Circuits* SC-9,

The author is at Intel Corporation, 5200 NE Elam Parkway, Hillsboro, OR 97124, USA. E-mail: paul.a.packan@intel.com

Enterprise hardware

Intel scientists find wall for Moore's Law

Last modified: December 1, 2003, 4:00 AM PST

By Michael Kanellos
Staff Writer, CNET News.com

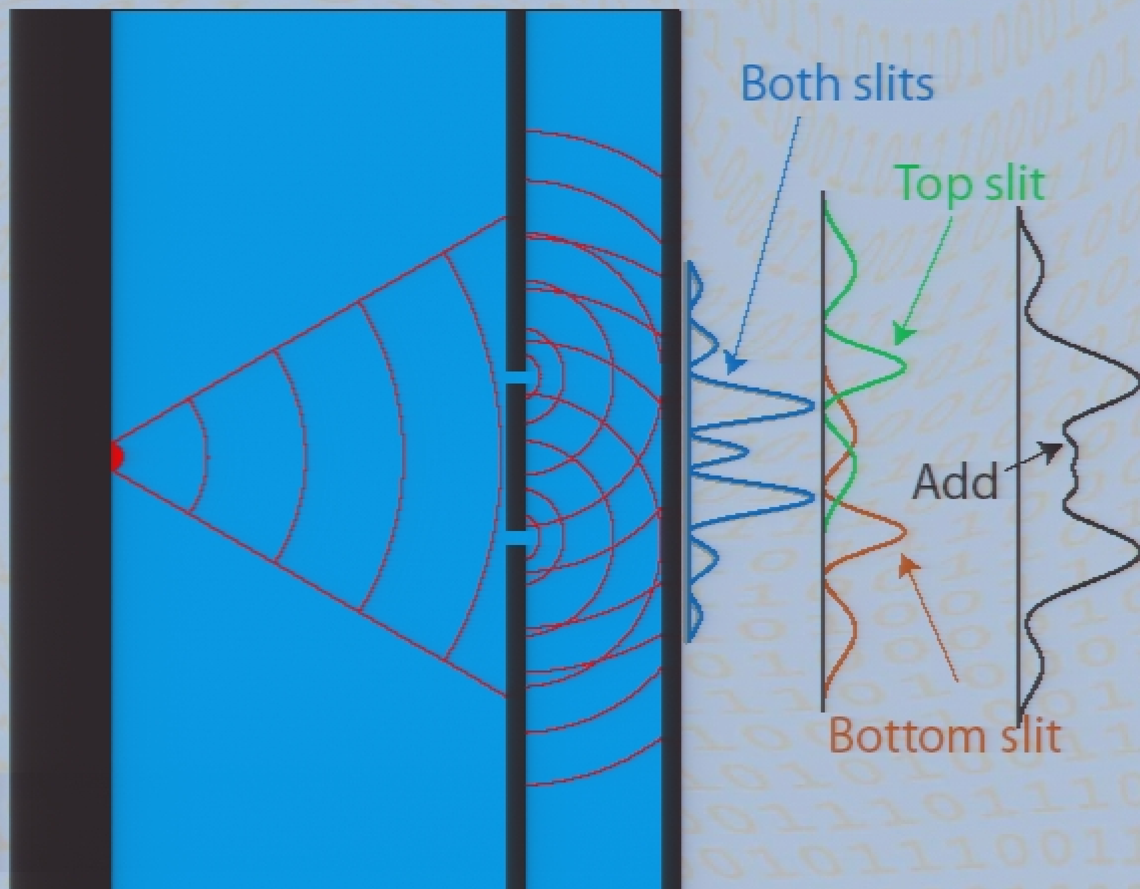
Moore's Law, as chip manufacturers generally refer to it today, is coming to an end, according to a recent research paper.

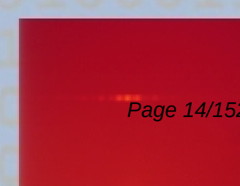
Granted, that end likely won't come for about two decades, but Intel researchers have recently published a paper theorizing that chipmakers will hit a wall when it comes to shrinking the size of transistors, one of the chief methods for making chips that are smaller, more powerful and cheaper than their predecessors.

Manufacturers will be able to produce chips on the 16-nanometer manufacturing process, expected by conservative estimates to arrive in 2018, and maybe one or two manufacturing processes after that, but that's it.

Basics of Quantum Mechanics

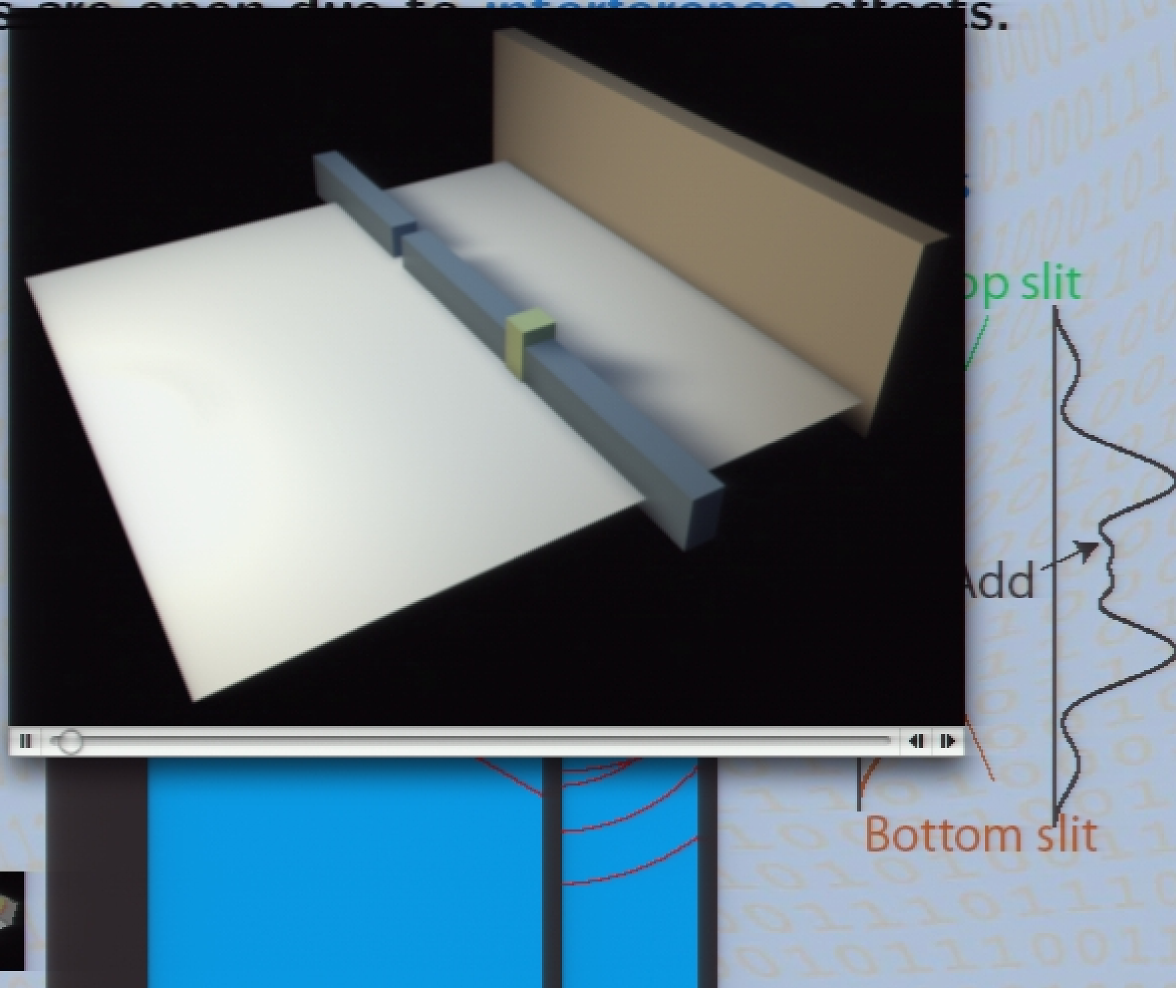
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

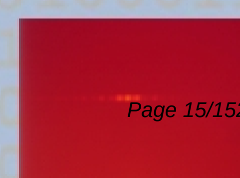




Basics of Quantum Mechanics

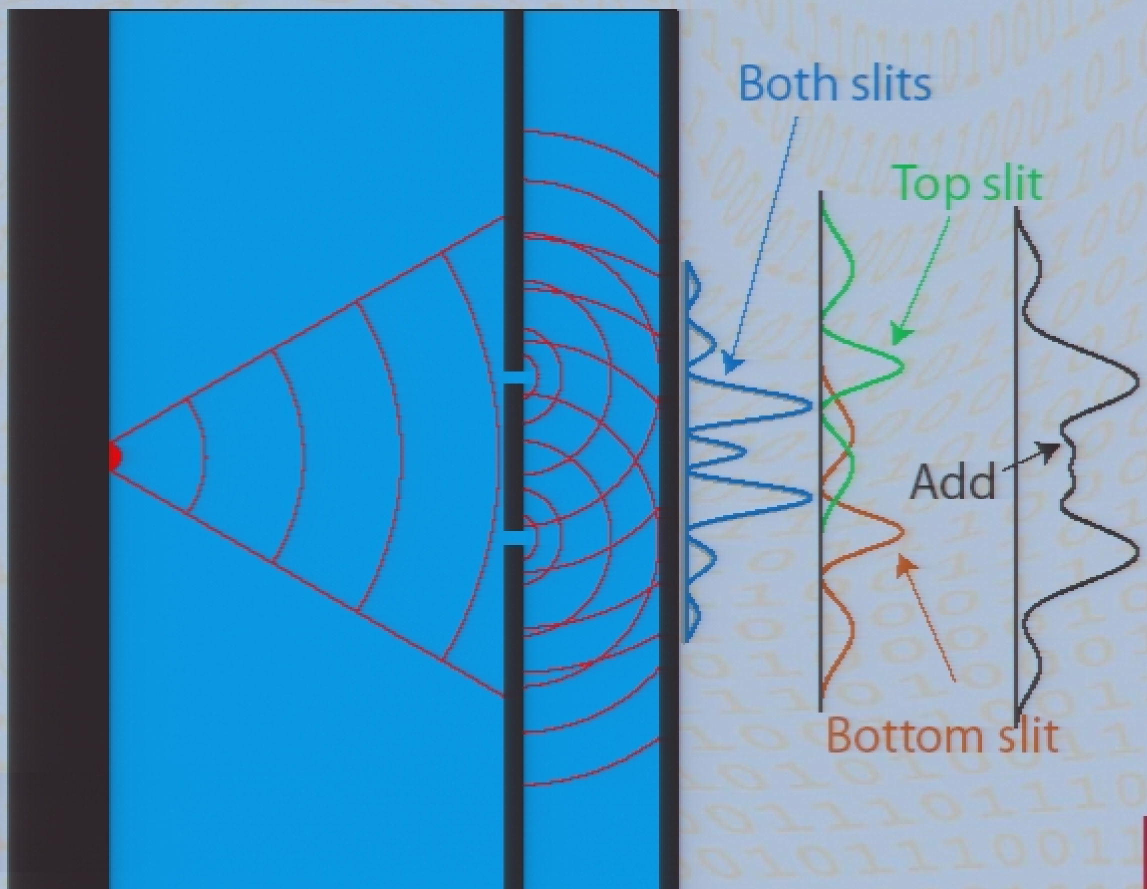
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

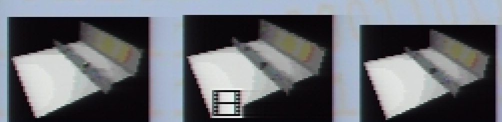




Basics of Quantum Mechanics

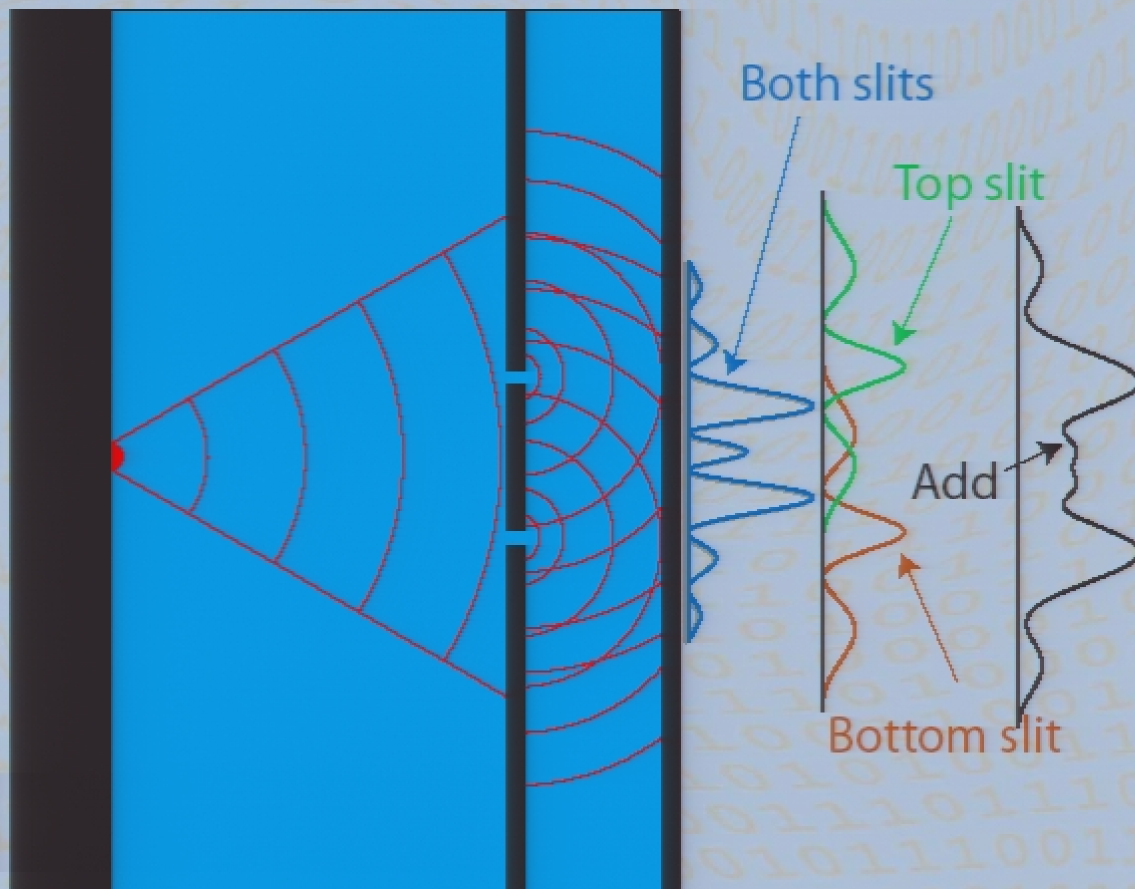
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

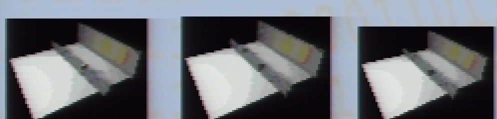




Basics of Quantum Mechanics

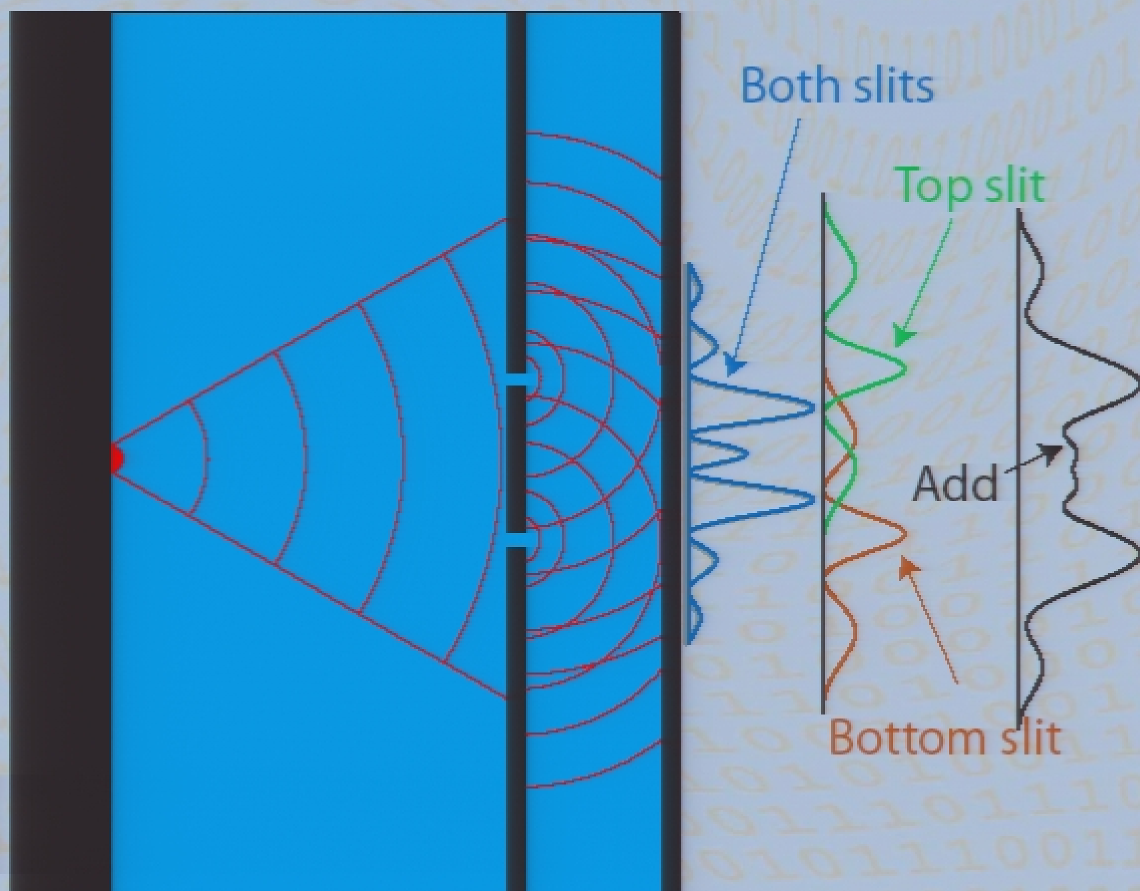
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





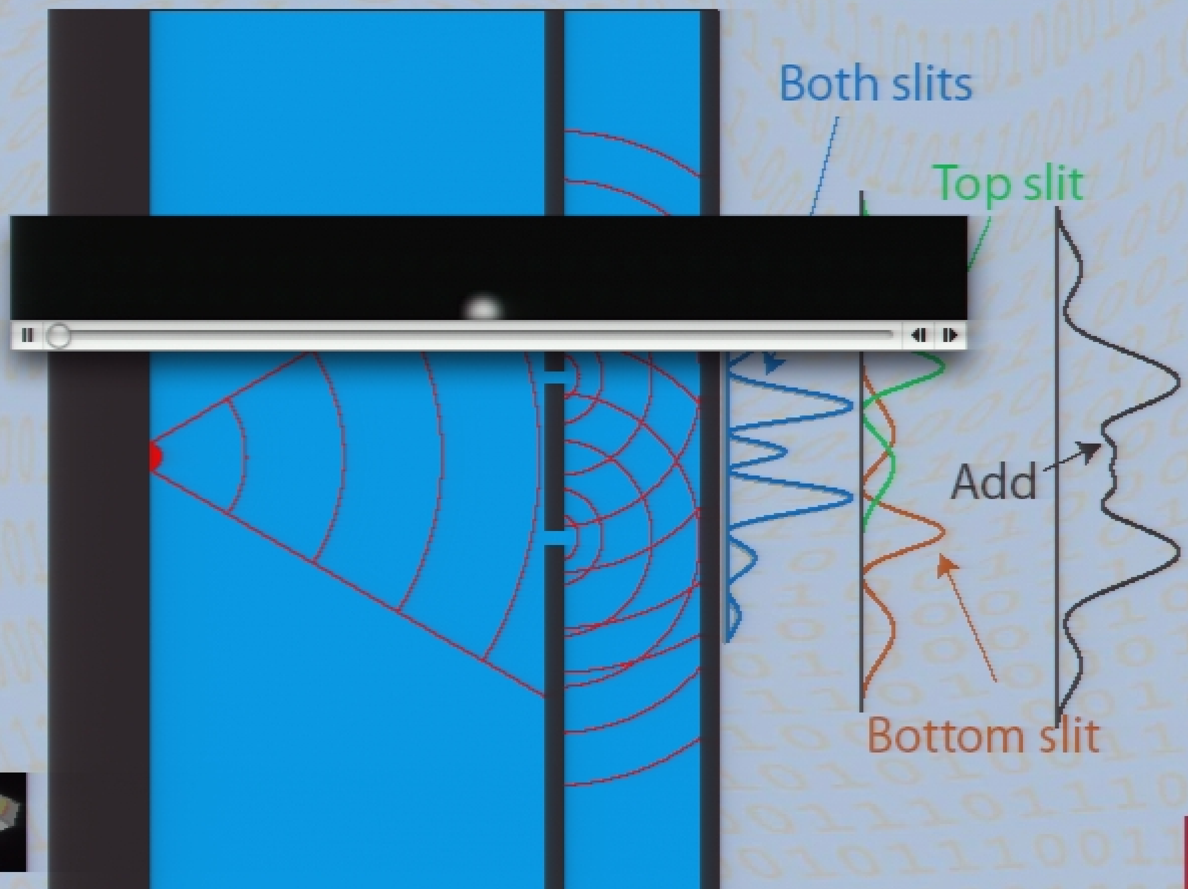
Basics of Quantum Mechanics

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.



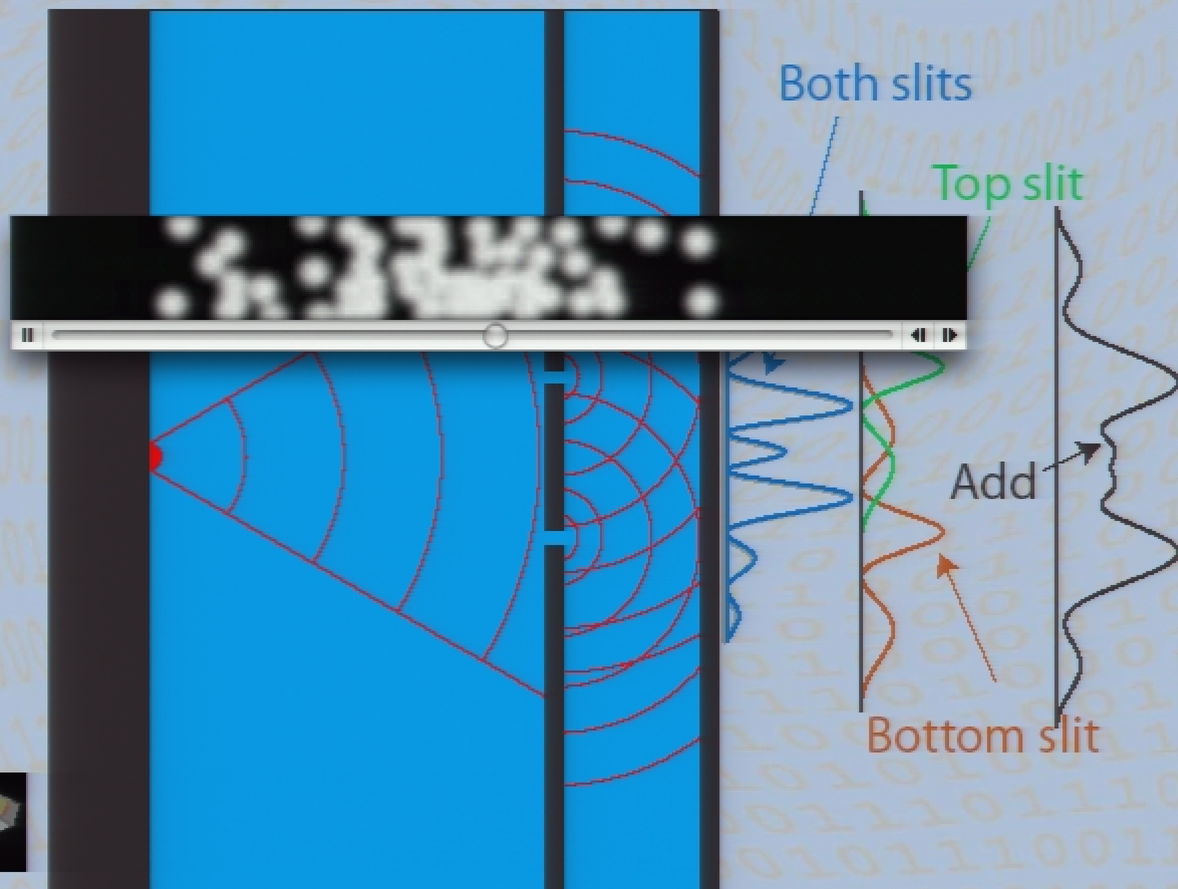
Basics of Quantum Mechanics

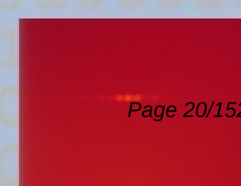
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

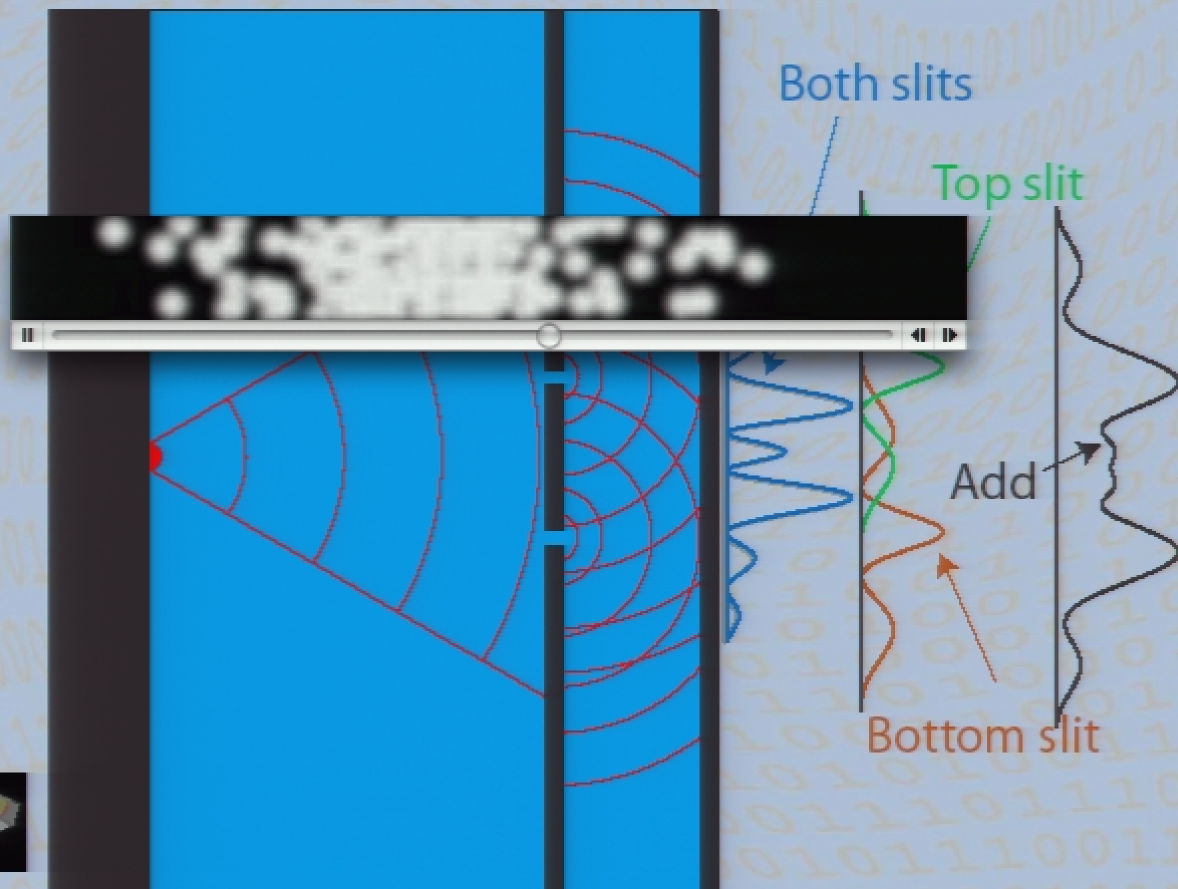
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

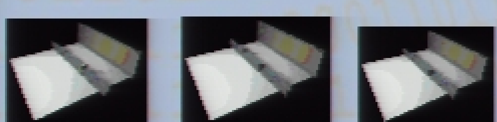




Basics of Quantum Mechanics

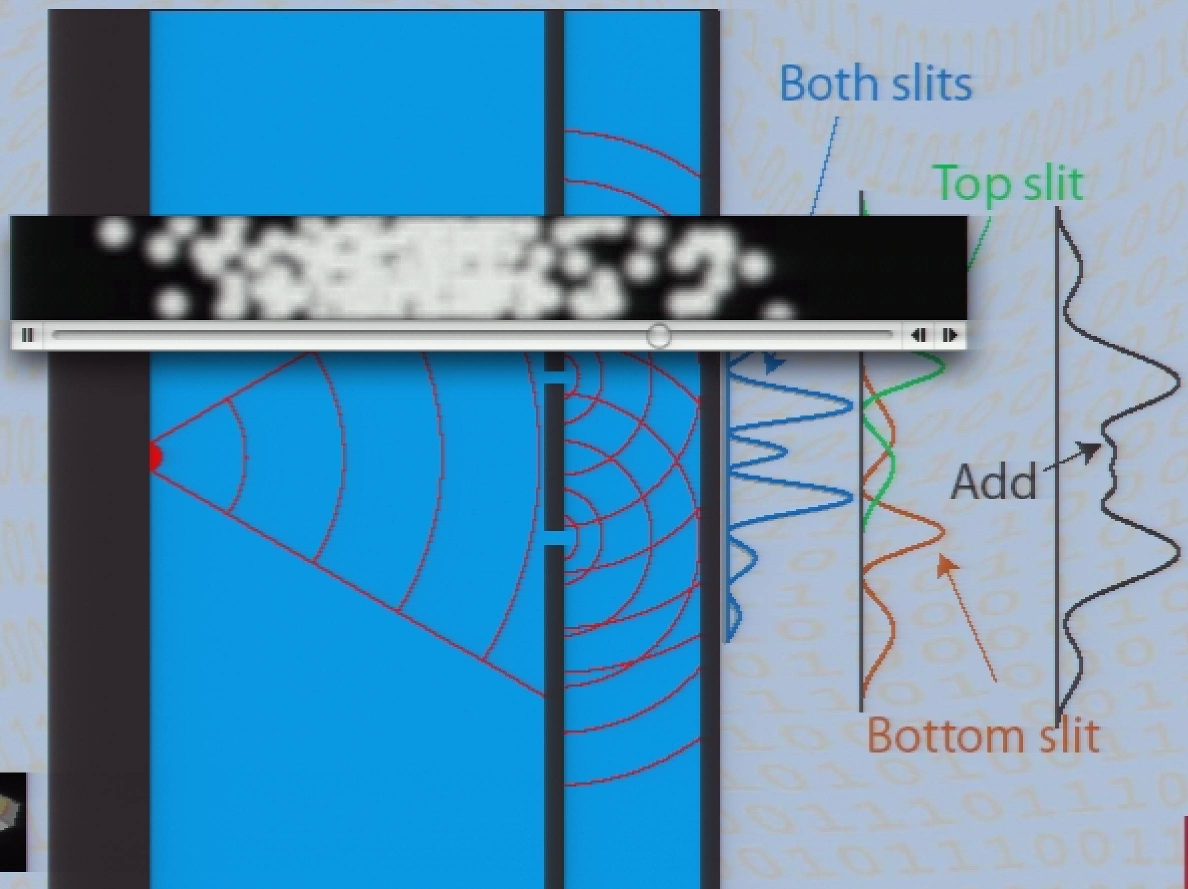
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

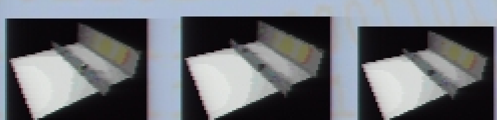




Basics of Quantum Mechanics

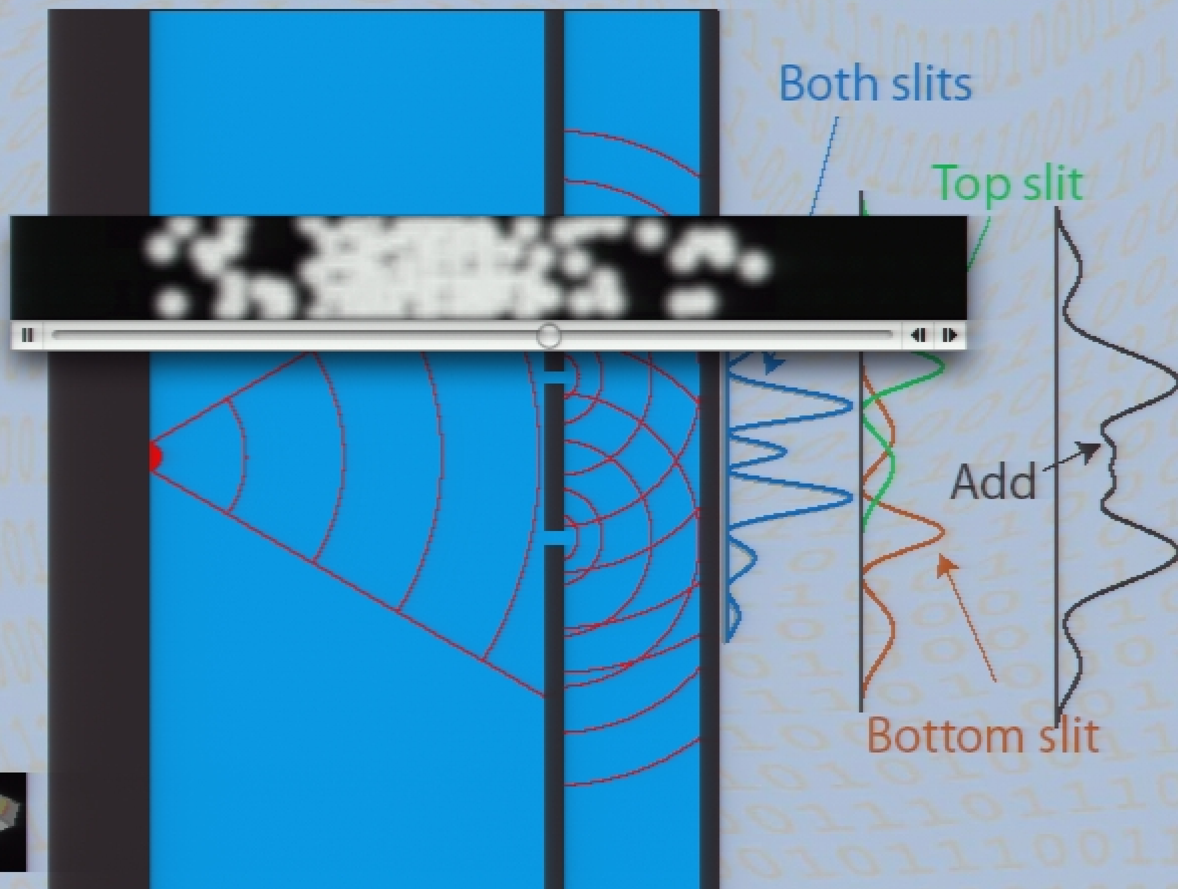
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

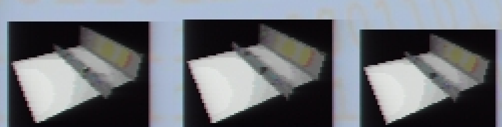




Basics of Quantum Mechanics

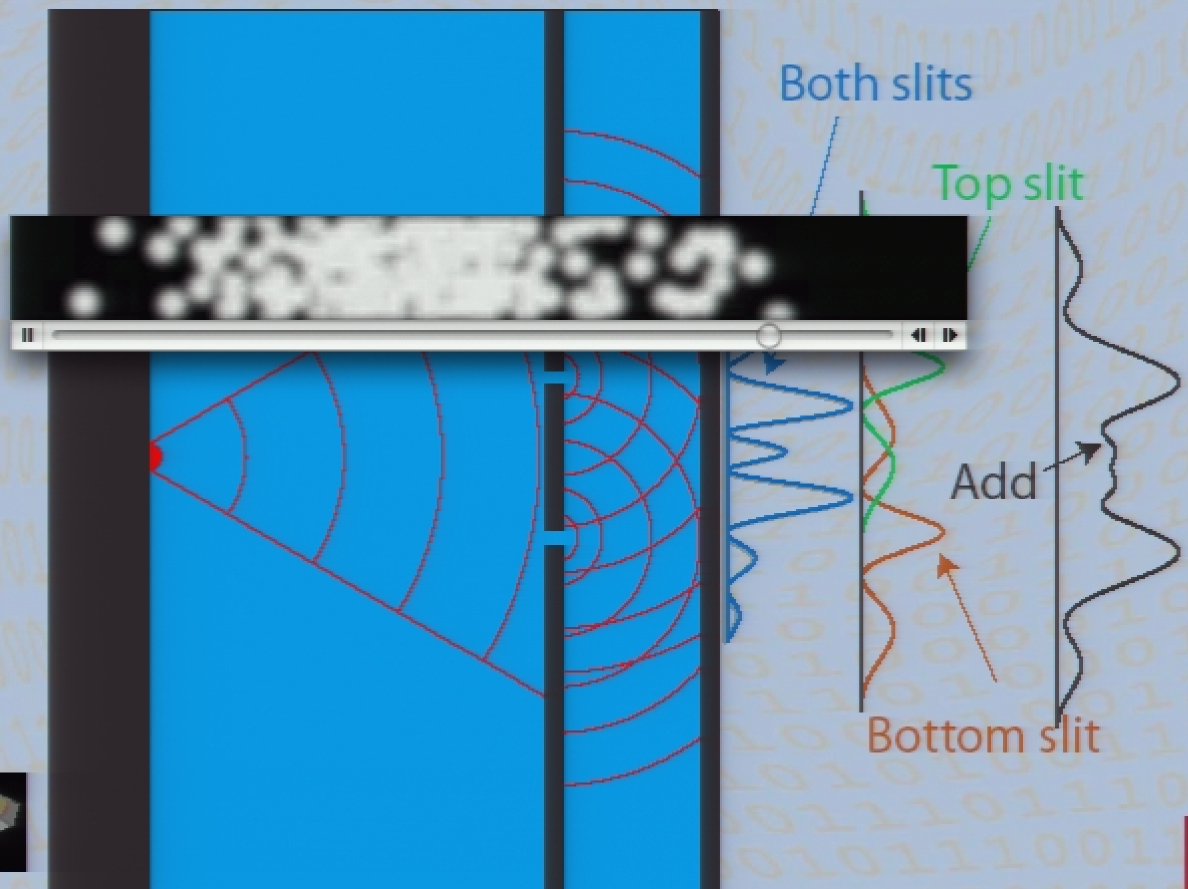
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

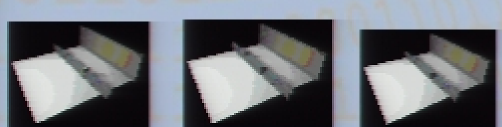




Basics of Quantum Mechanics

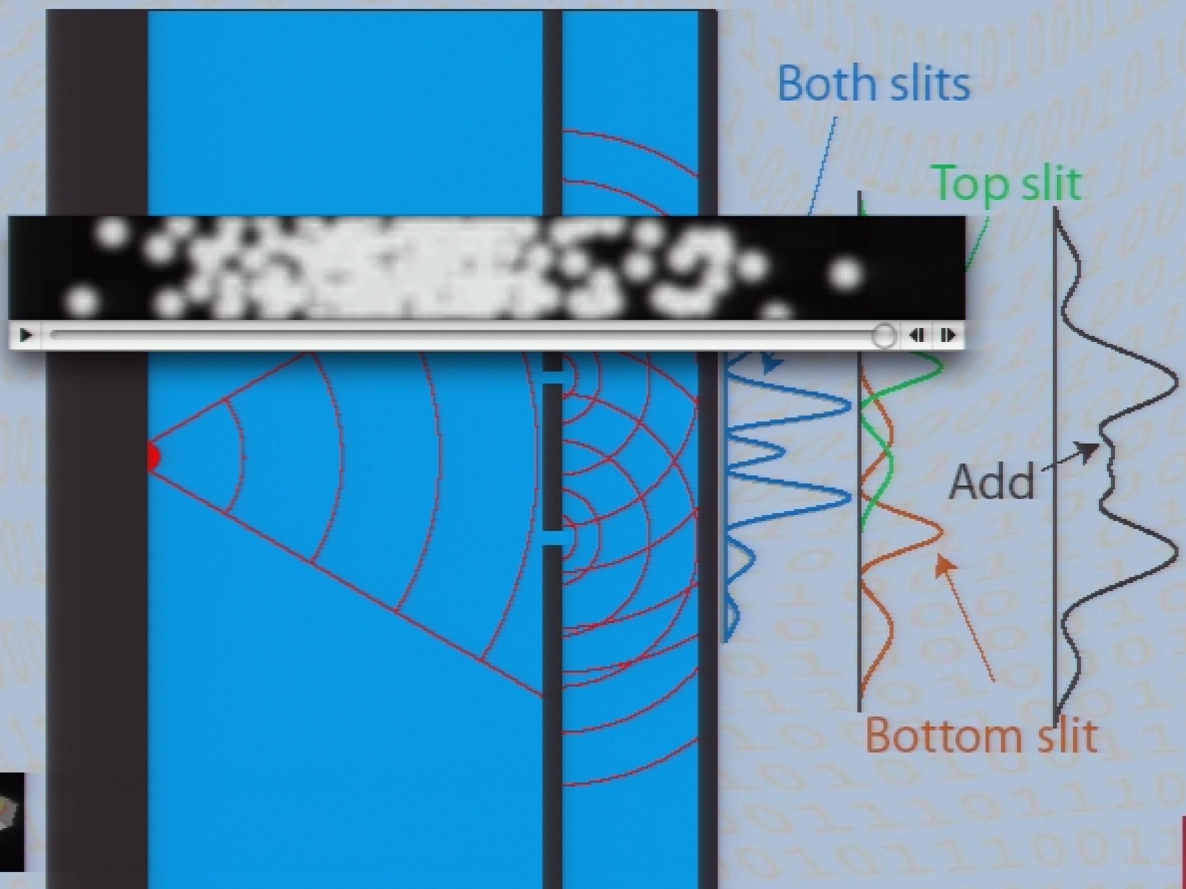
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

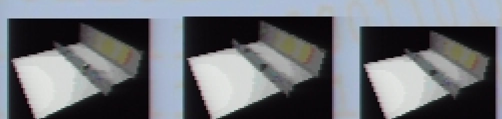




Basics of Quantum Mechanics

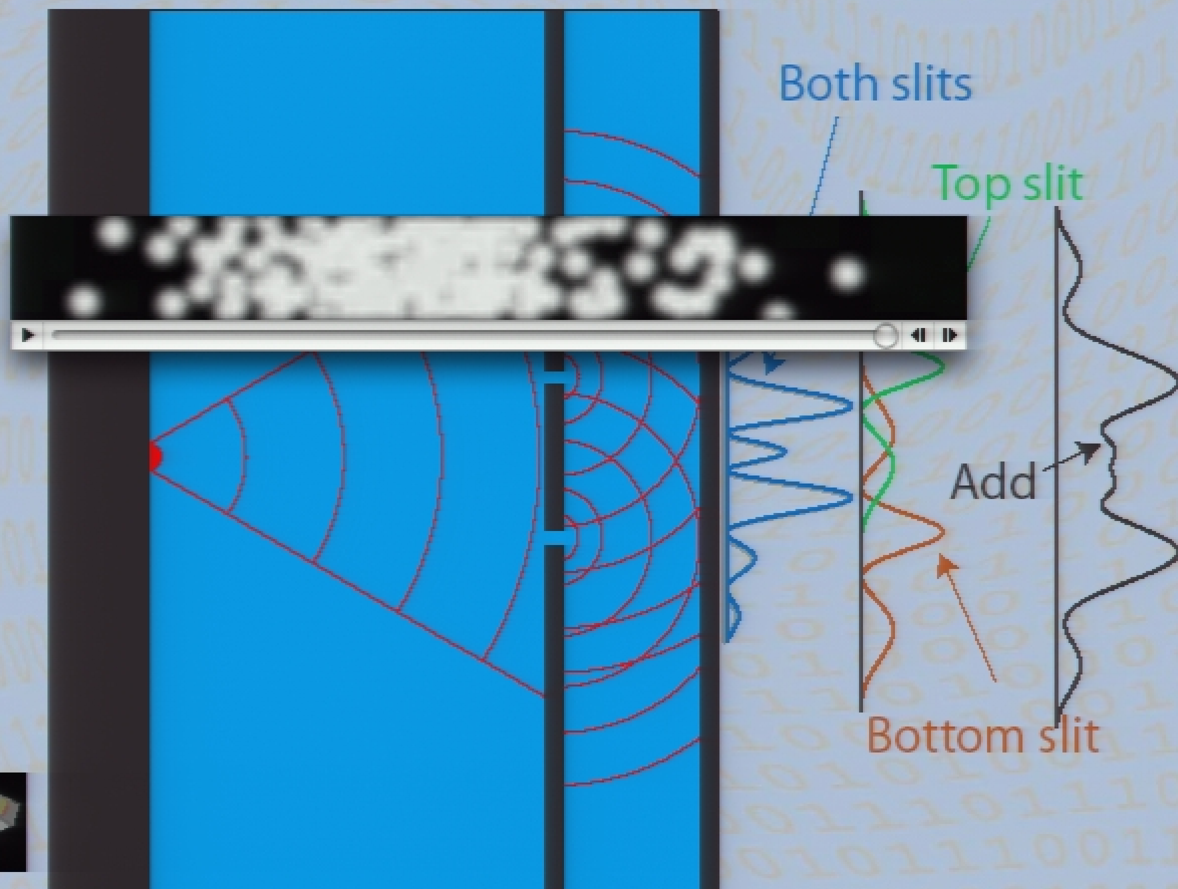
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

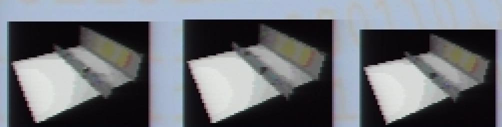




Basics of Quantum Mechanics

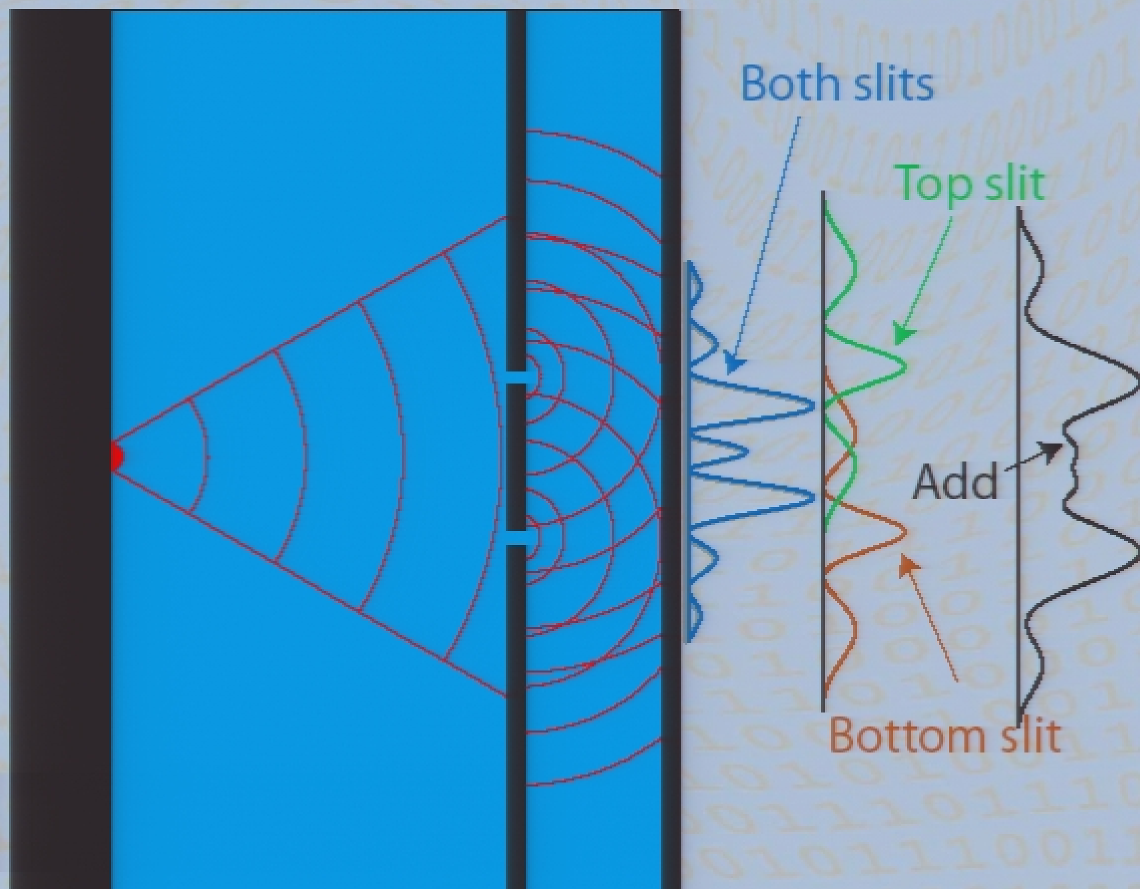
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

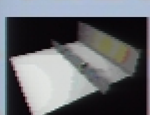




Basics of Quantum Mechanics

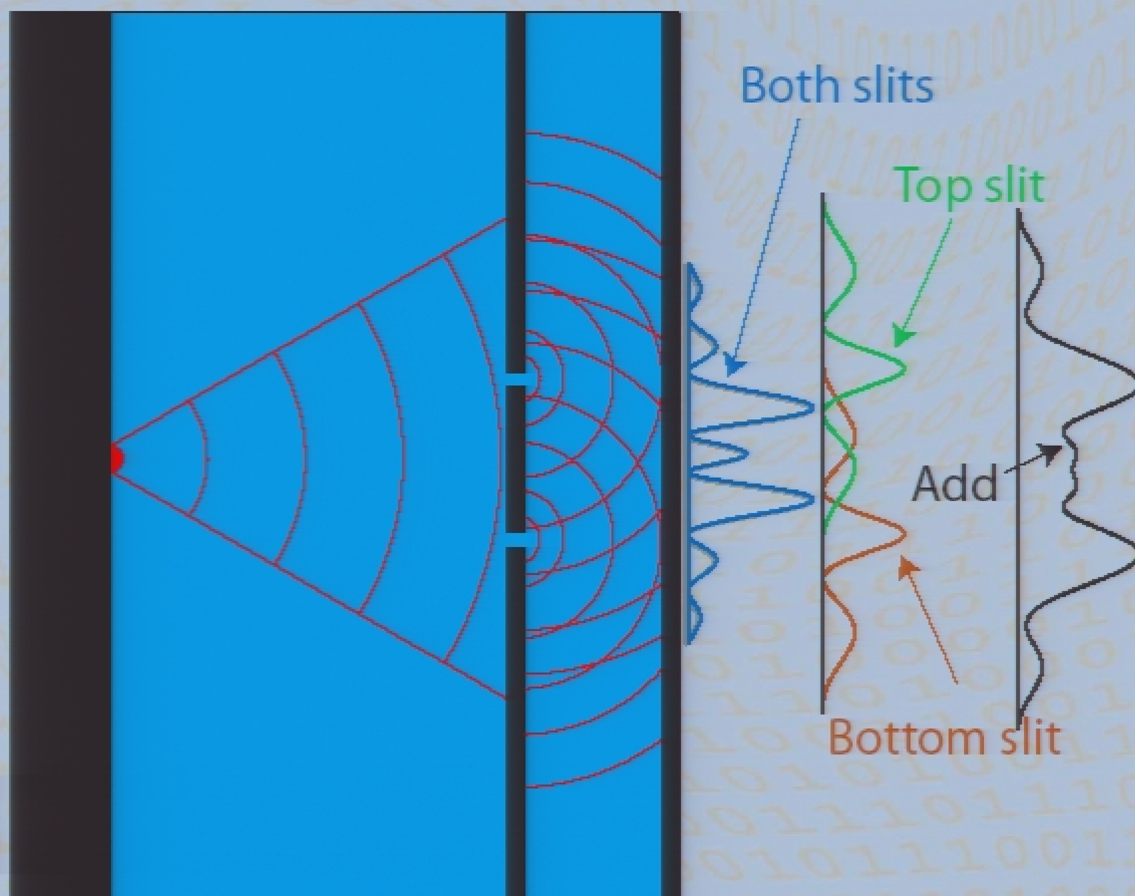
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





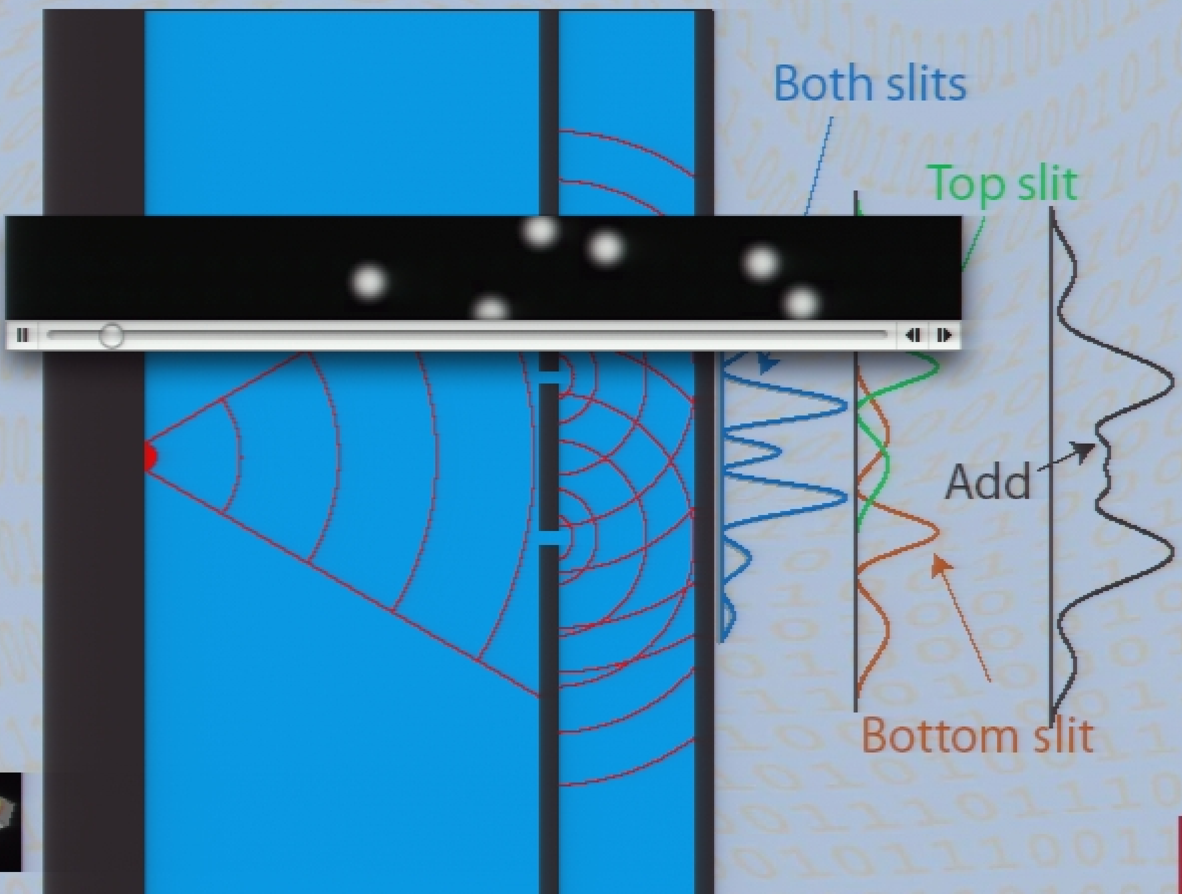
Basics of Quantum Mechanics

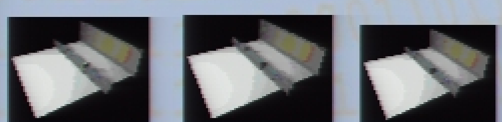
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

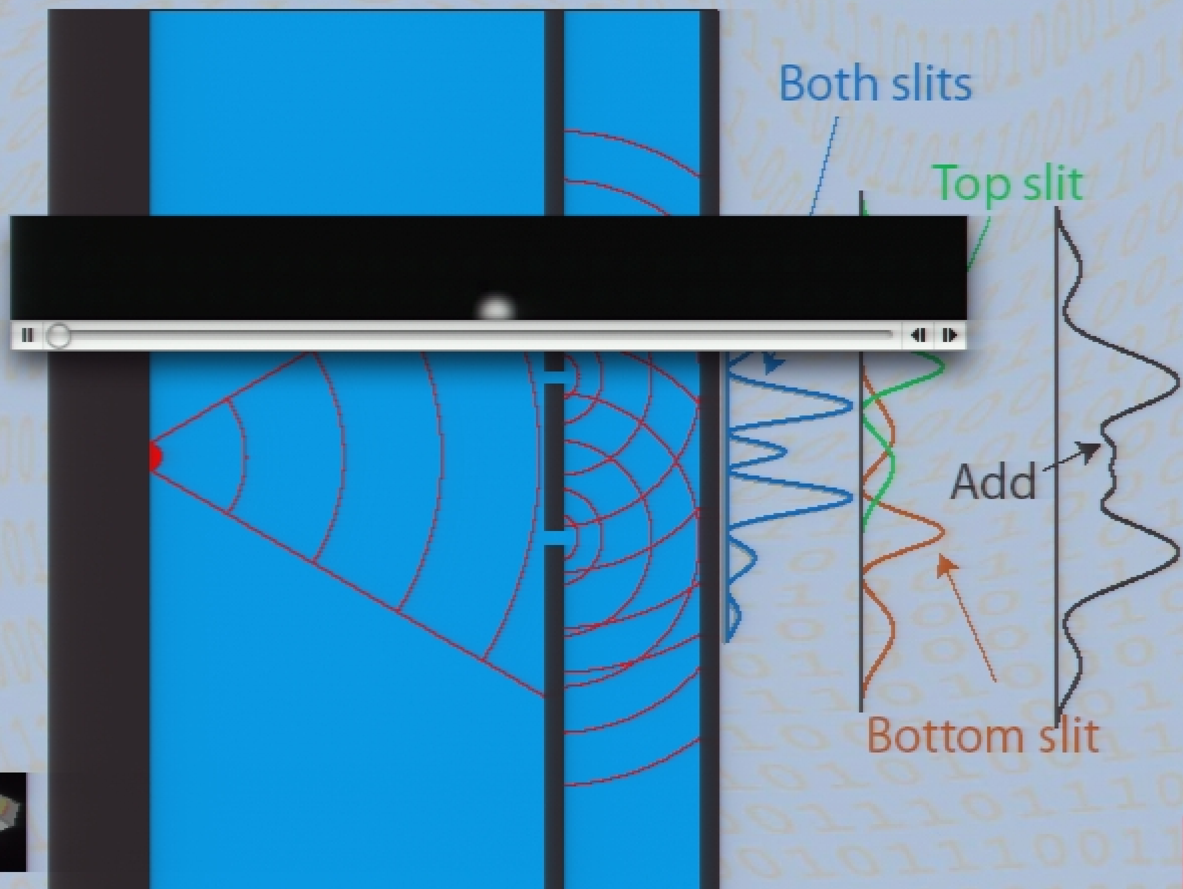
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

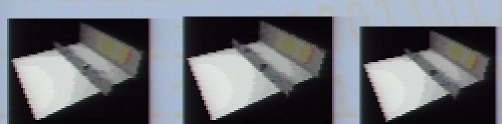




Basics of Quantum Mechanics

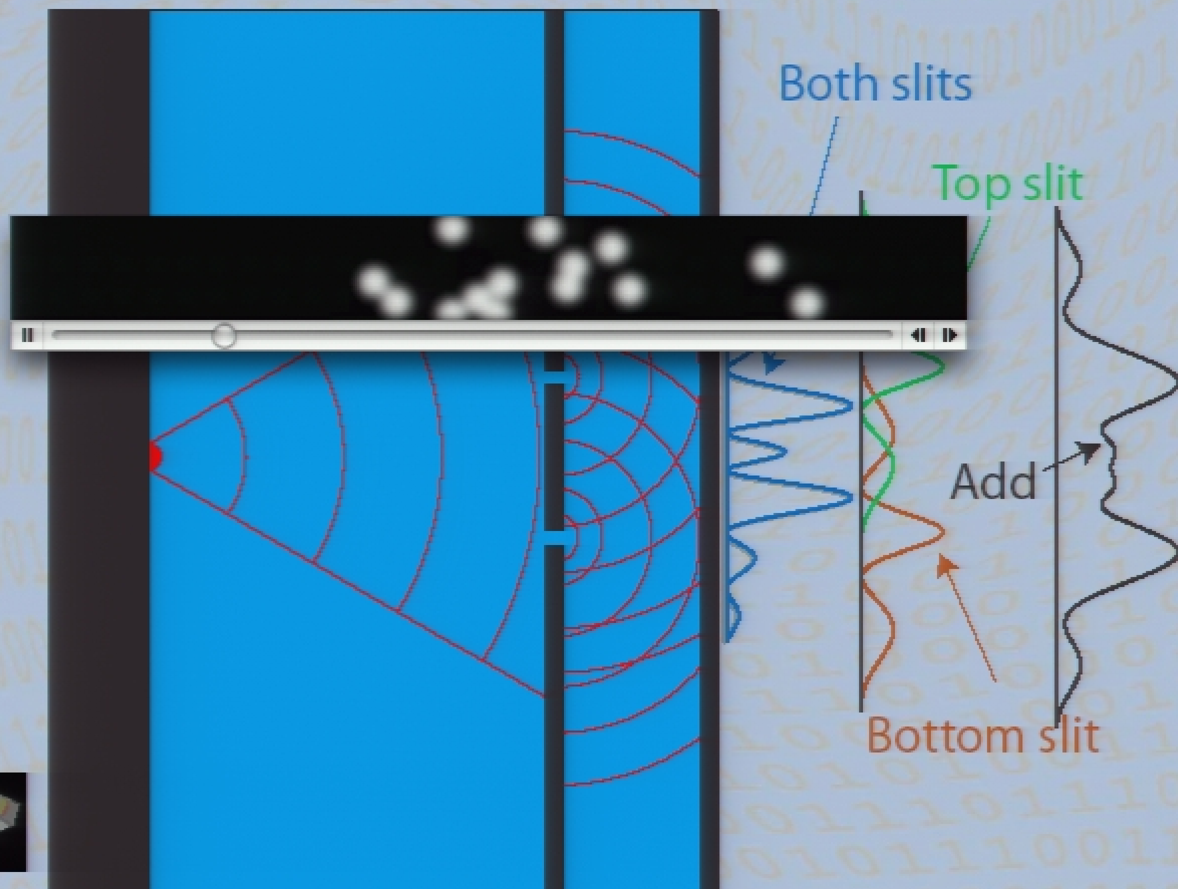
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

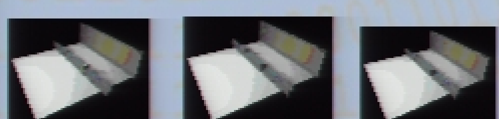




Basics of Quantum Mechanics

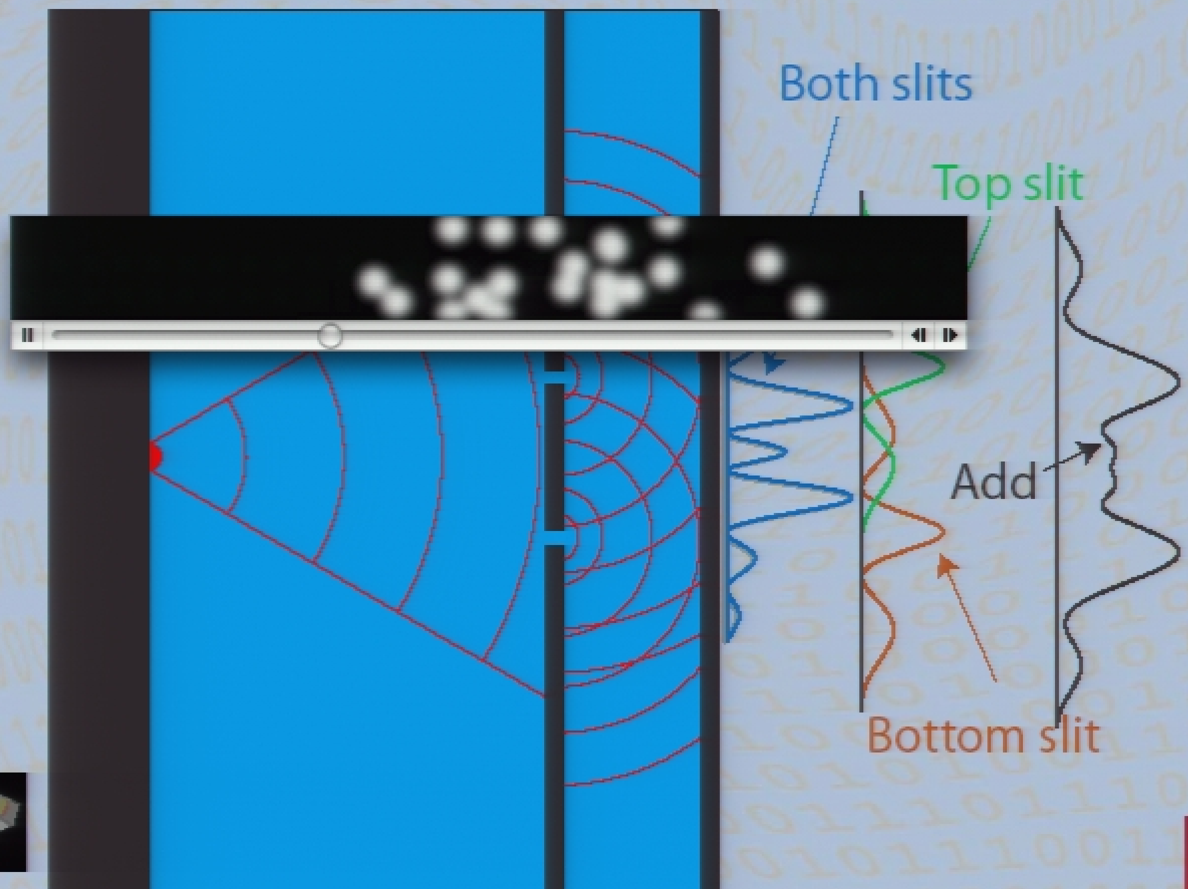
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

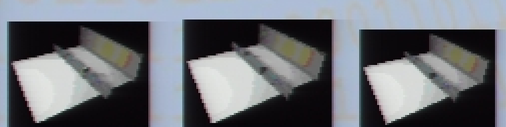




Basics of Quantum Mechanics

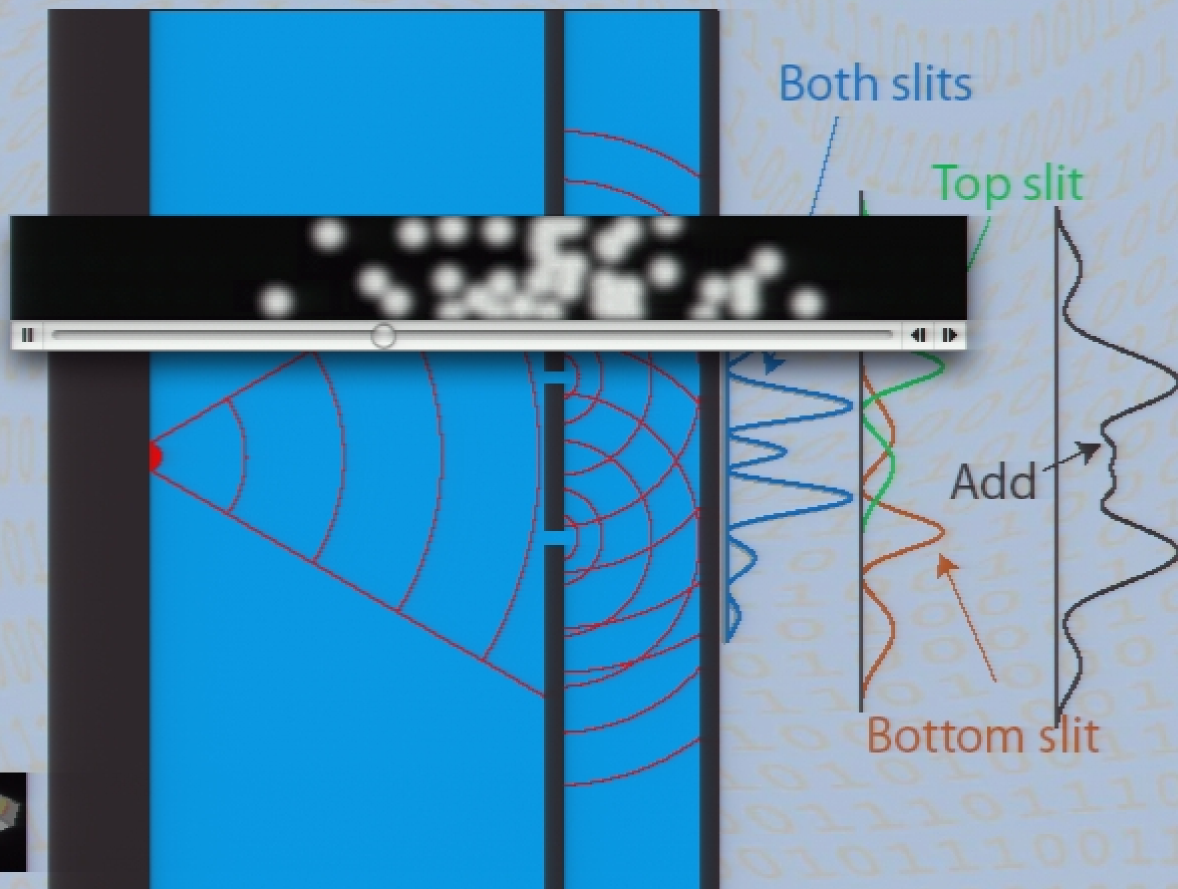
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

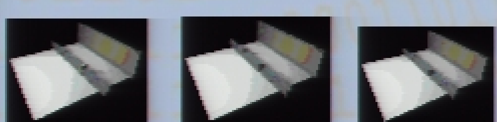




Basics of Quantum Mechanics

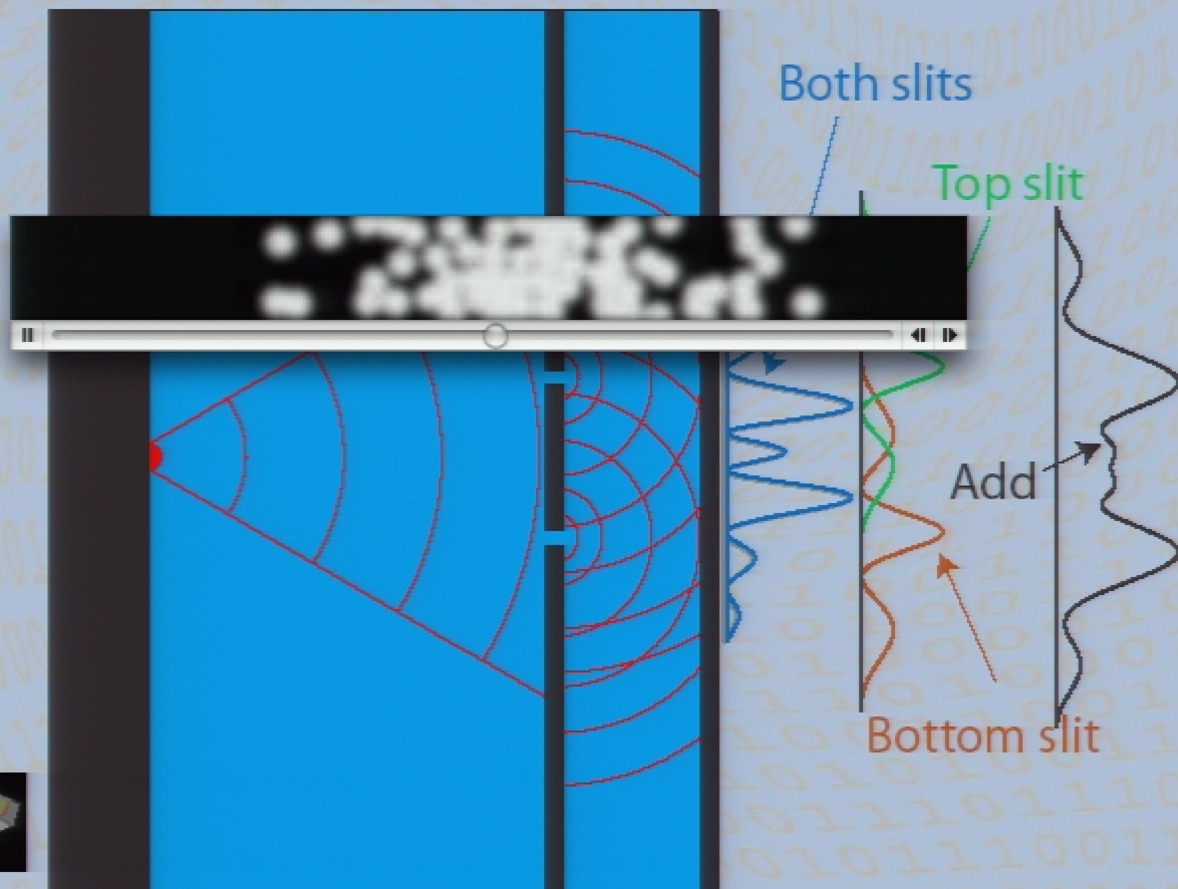
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

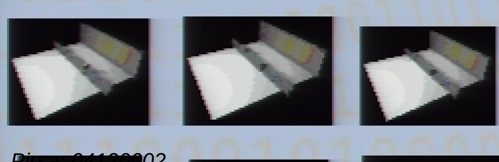


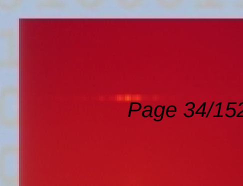


Basics of Quantum Mechanics

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.

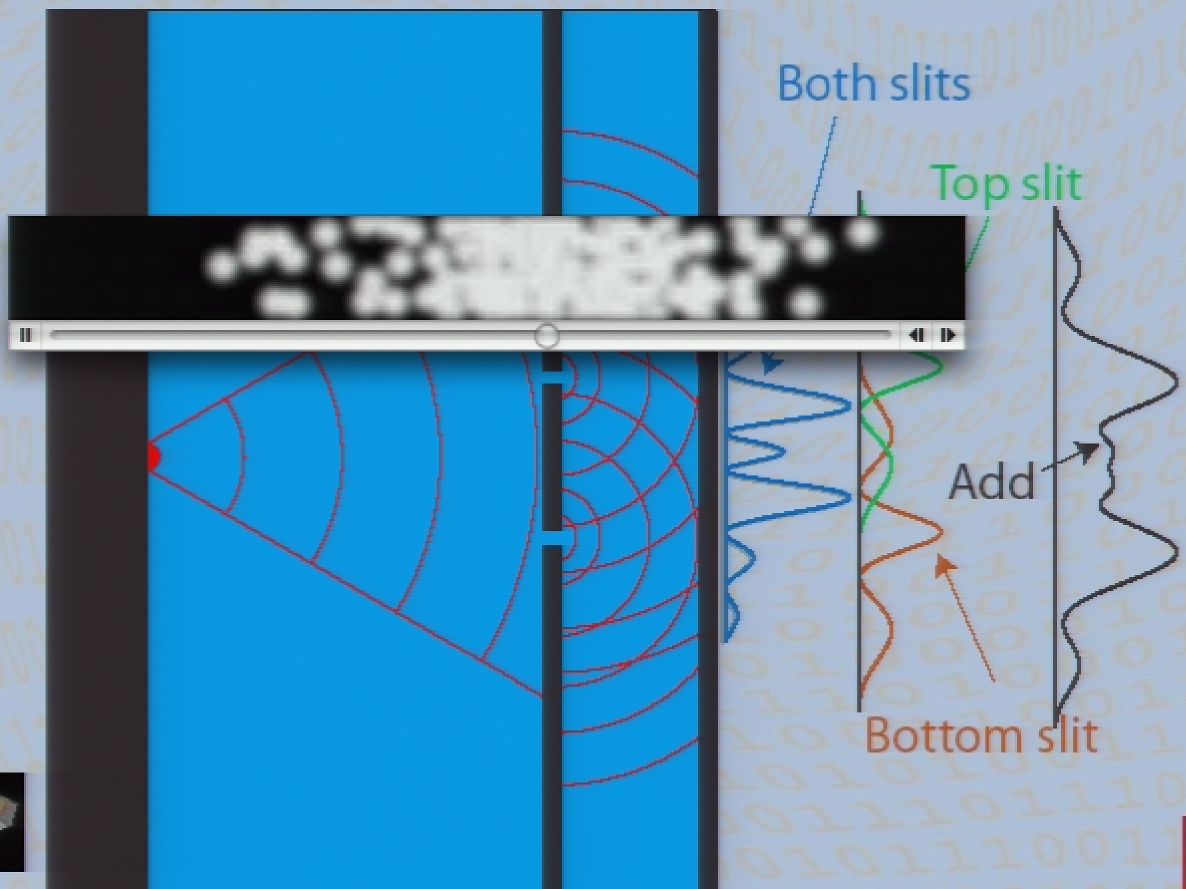


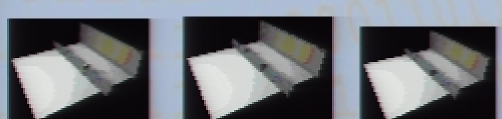




Basics of Quantum Mechanics

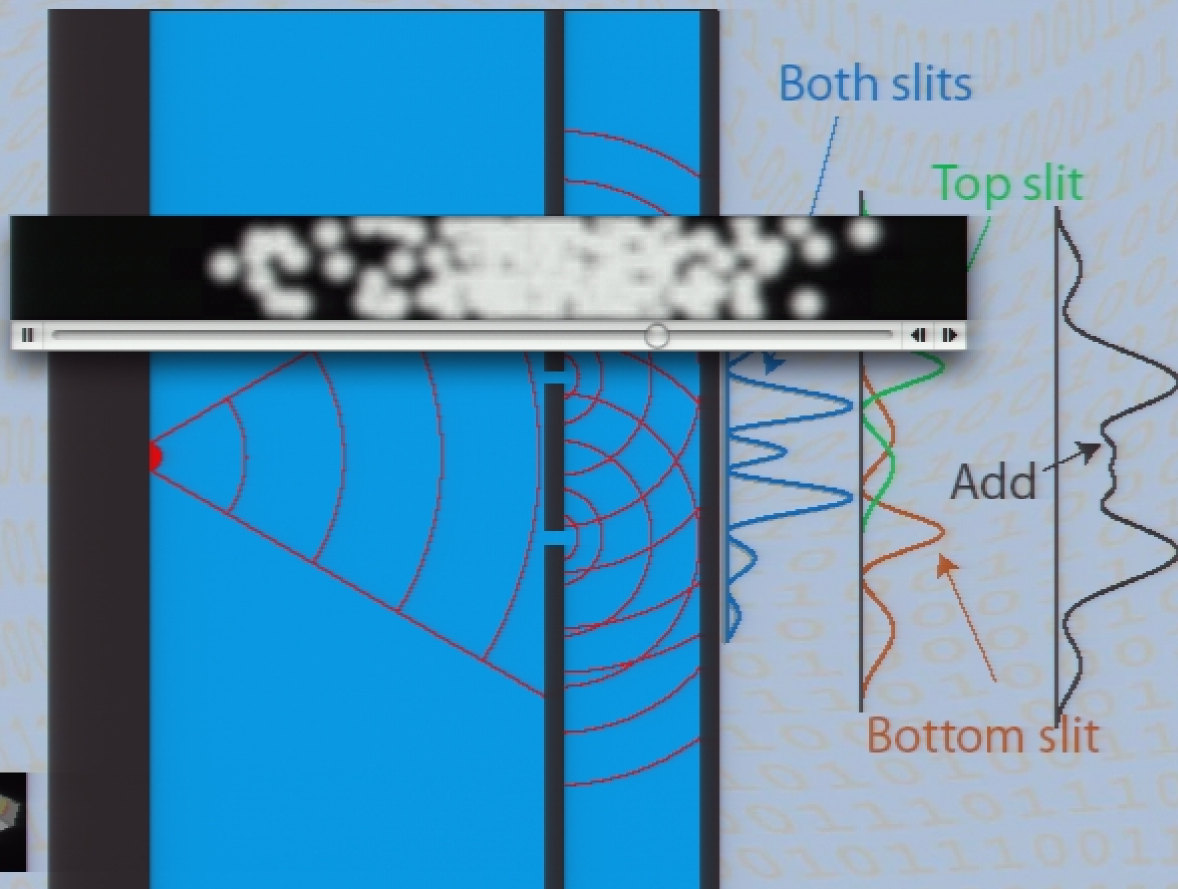
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

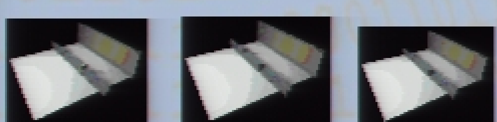




Basics of Quantum Mechanics

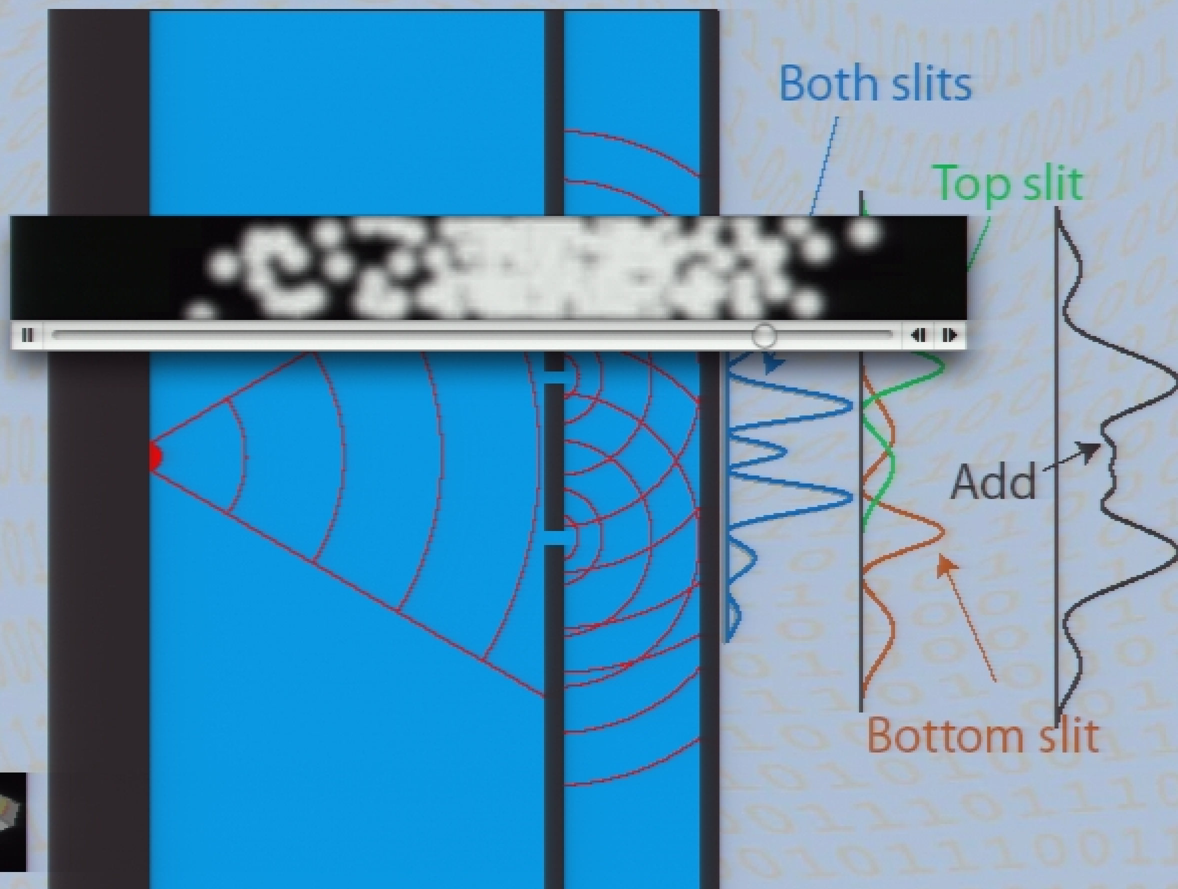
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

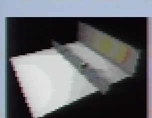


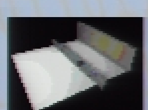


Basics of Quantum Mechanics

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.

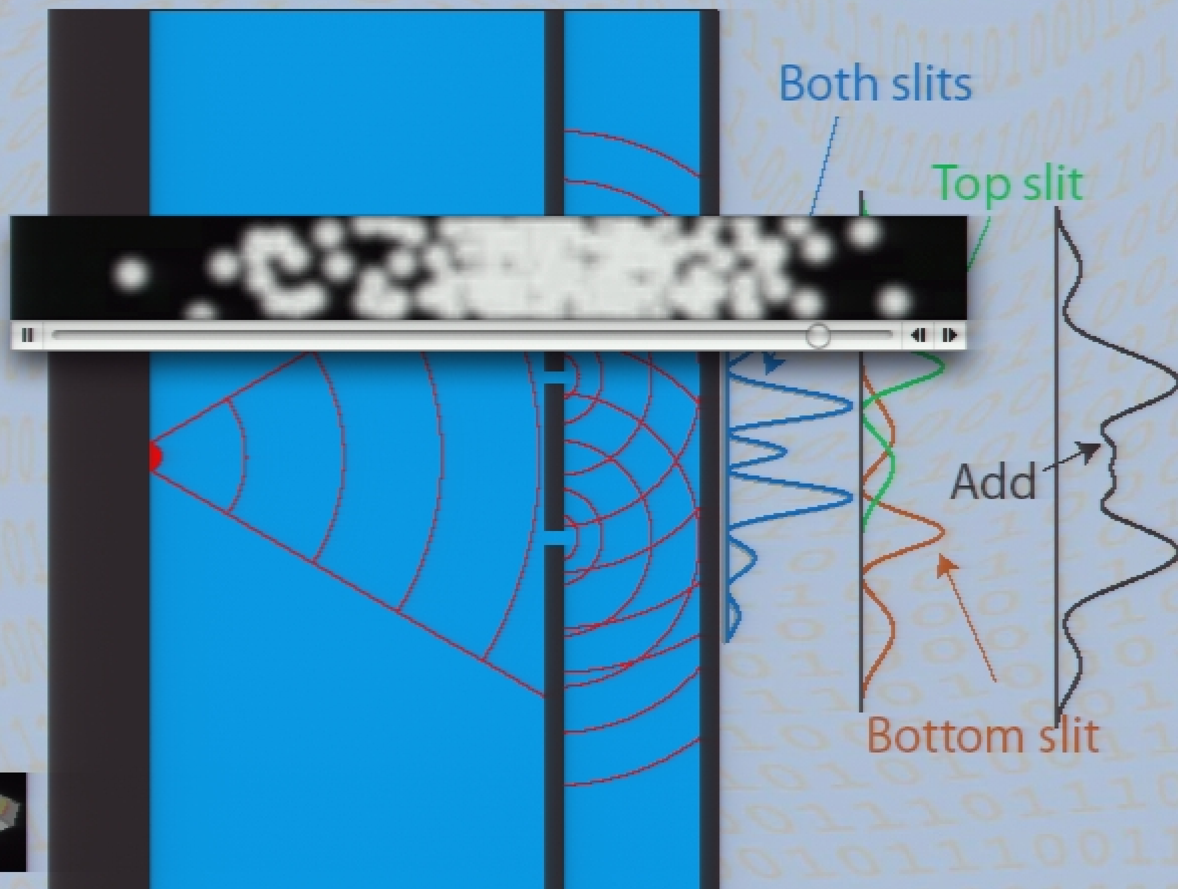






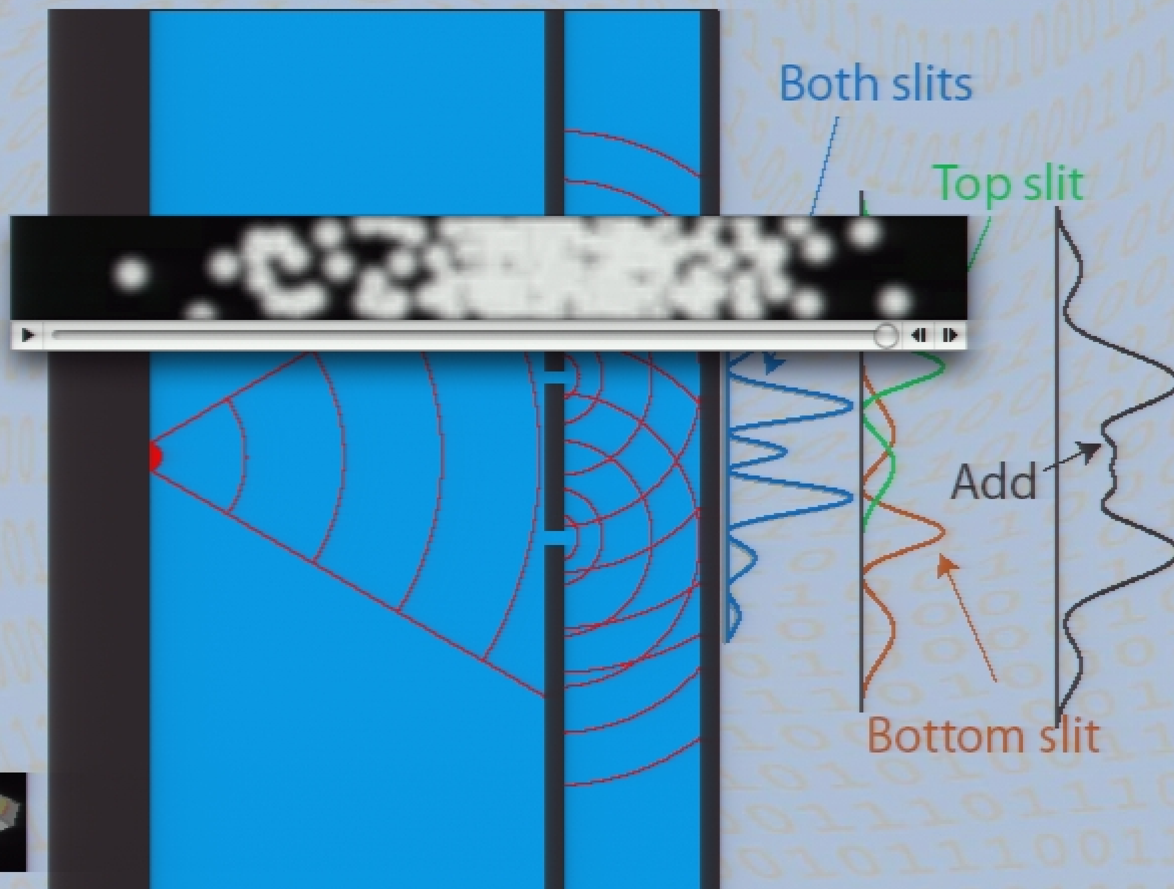
Basics of Quantum Mechanics

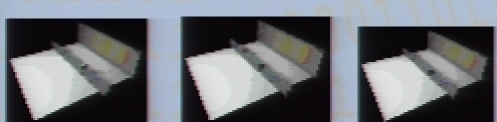
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

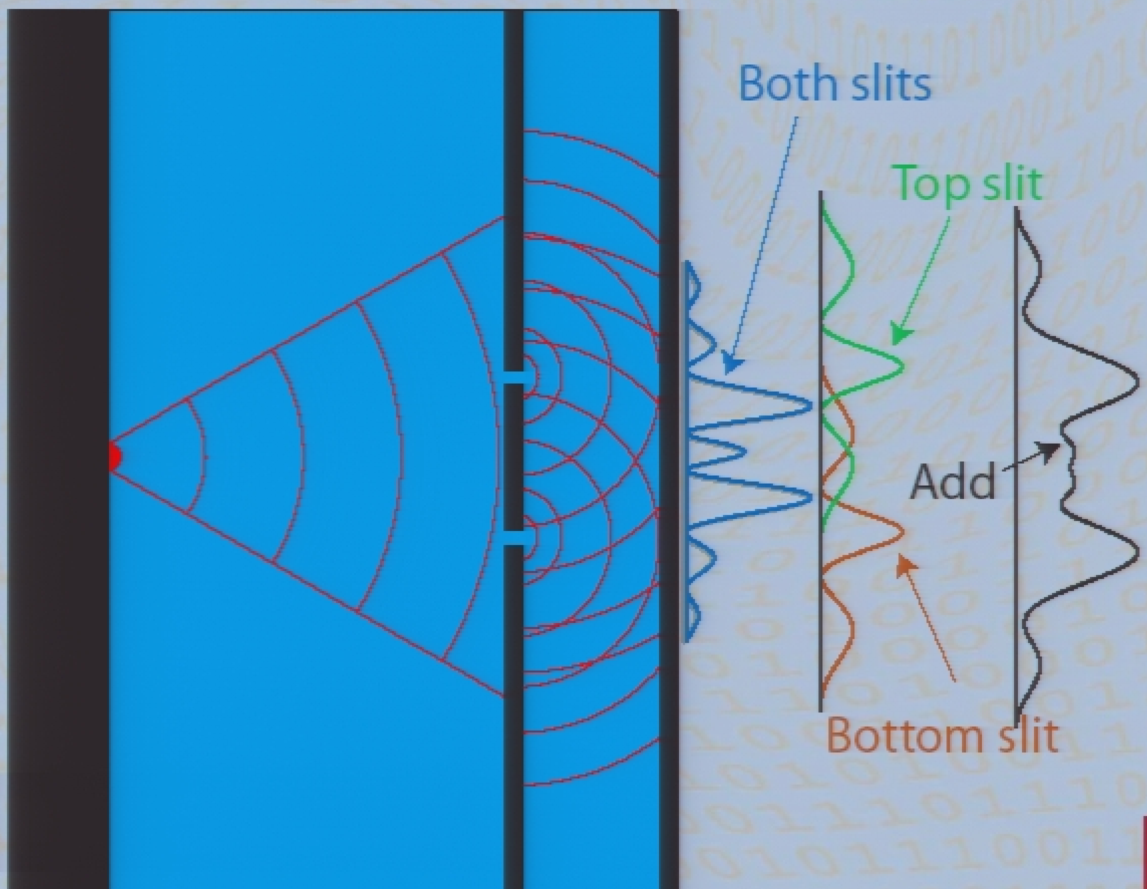
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





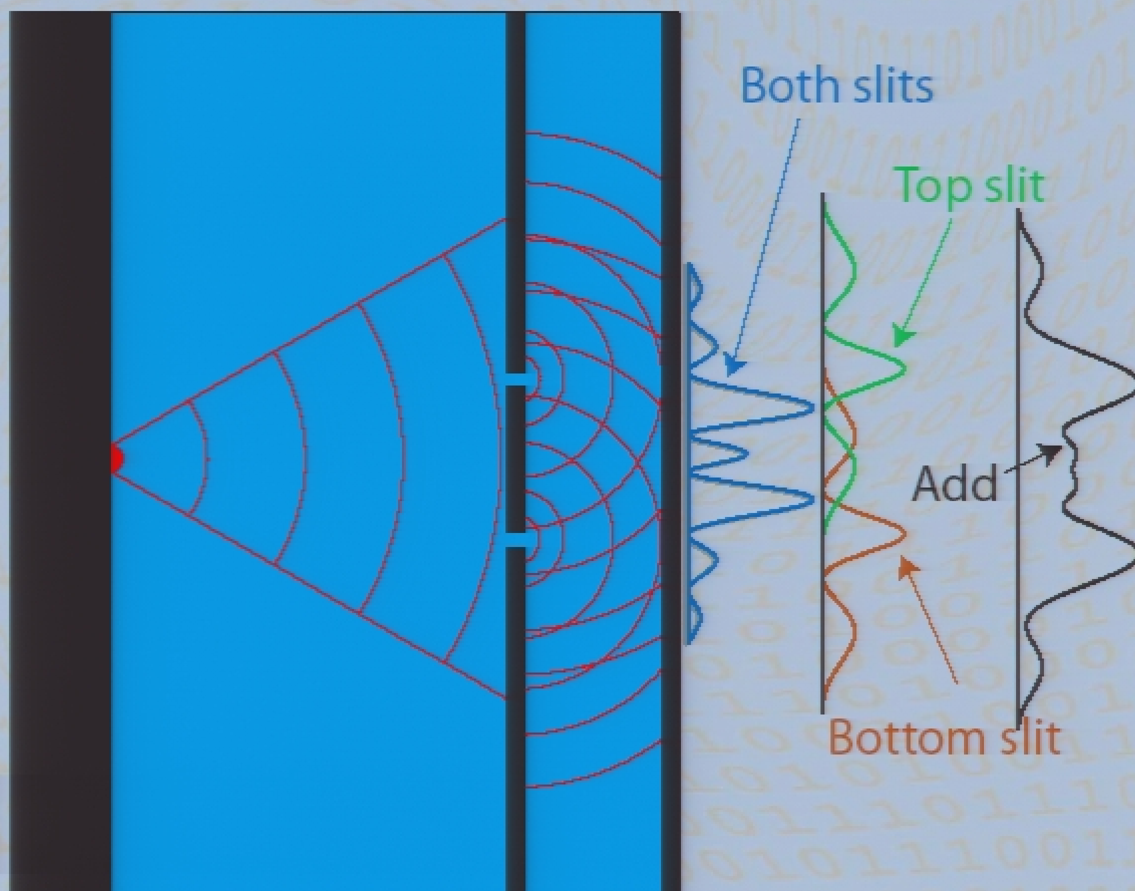
Basics of Quantum Mechanics

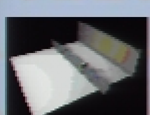
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

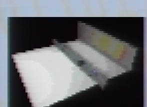


Basics of Quantum Mechanics

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.

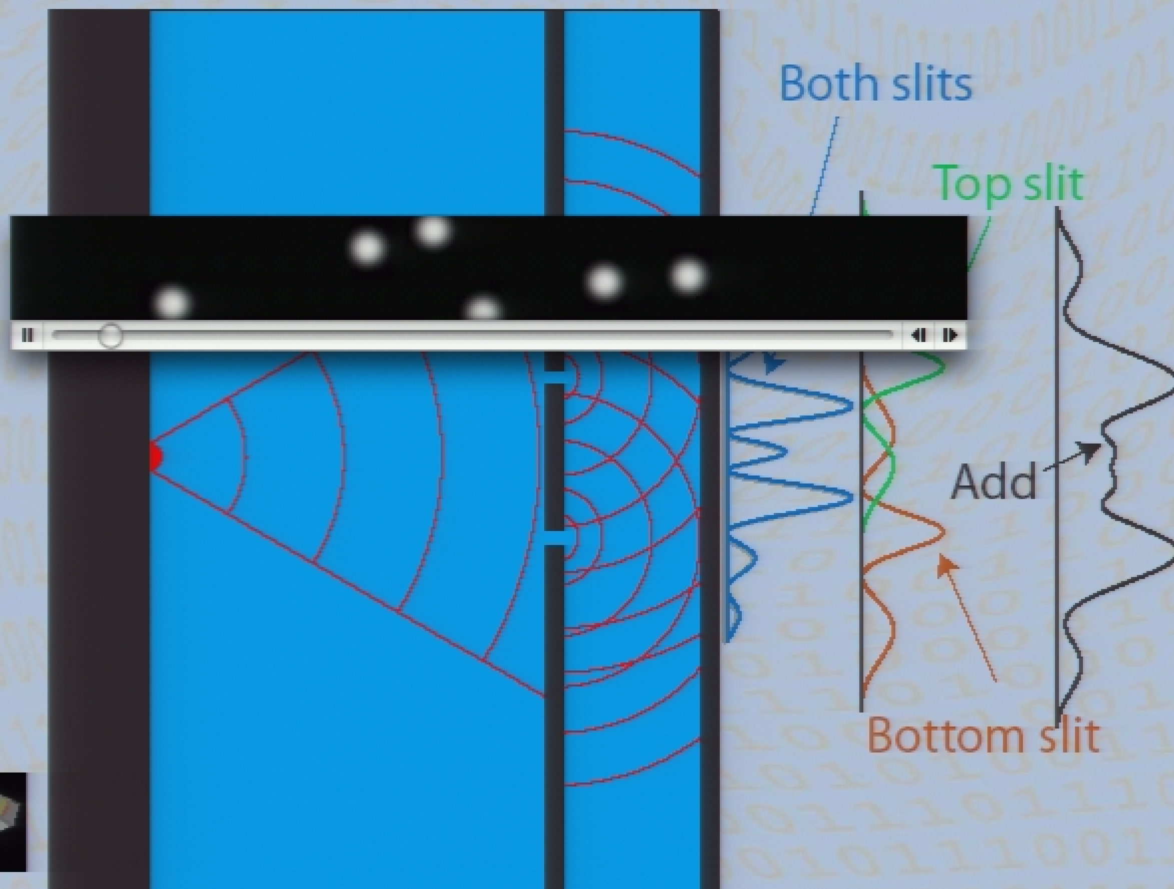






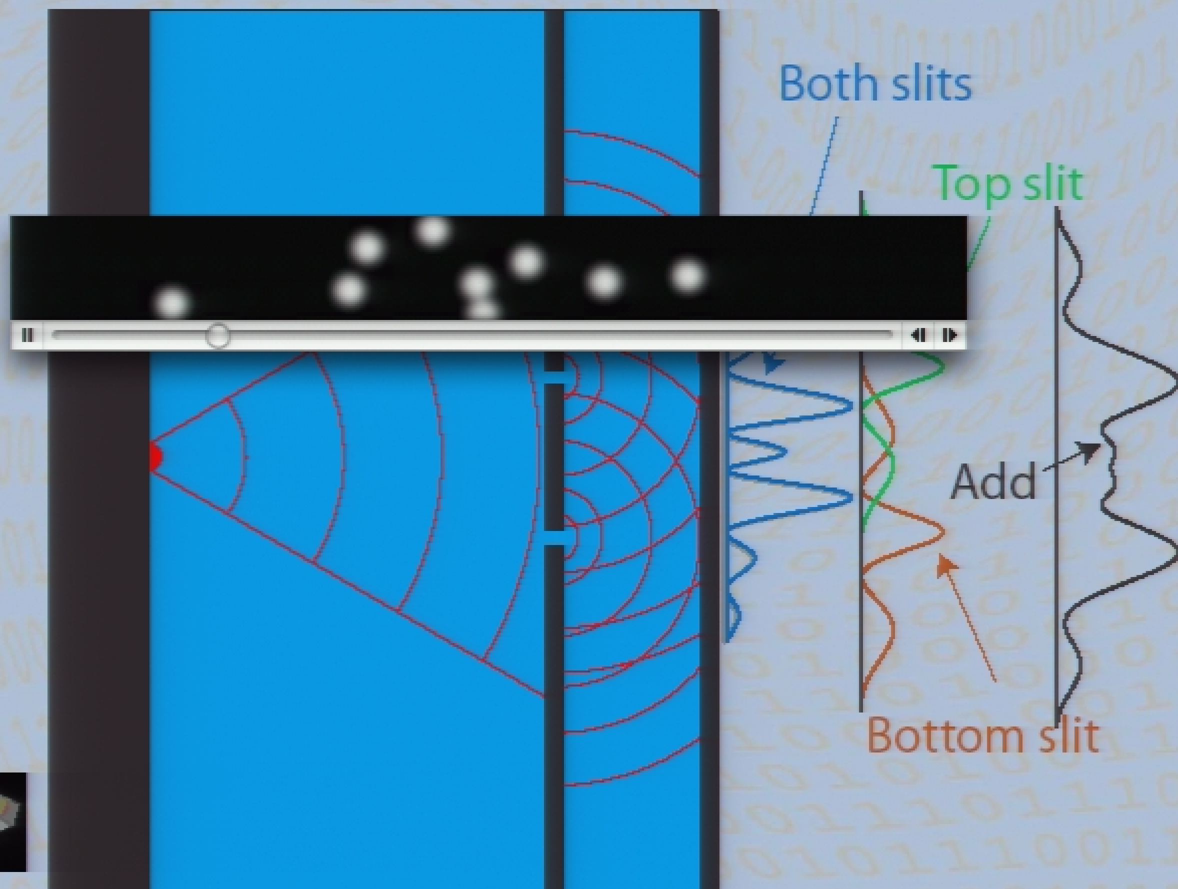
Basics of Quantum Mechanics

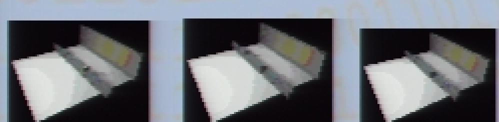
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

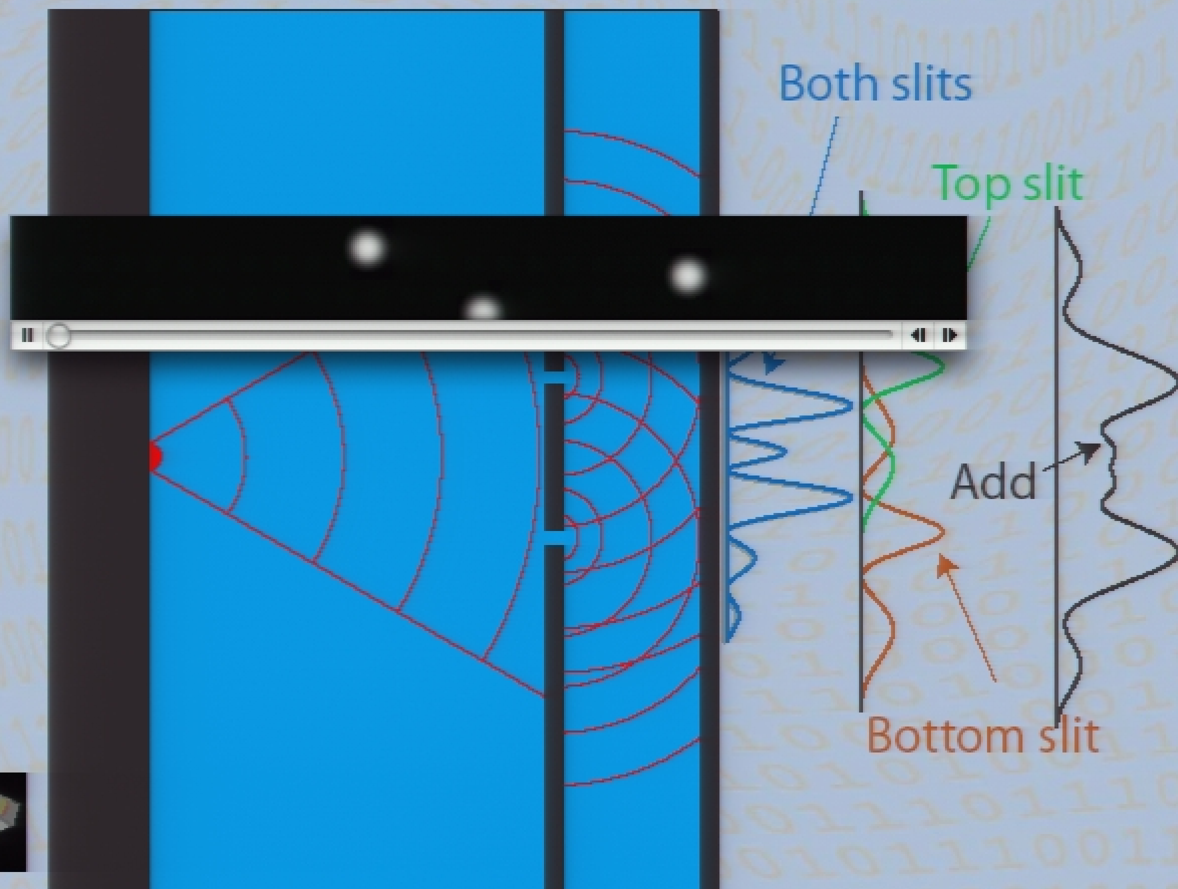
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





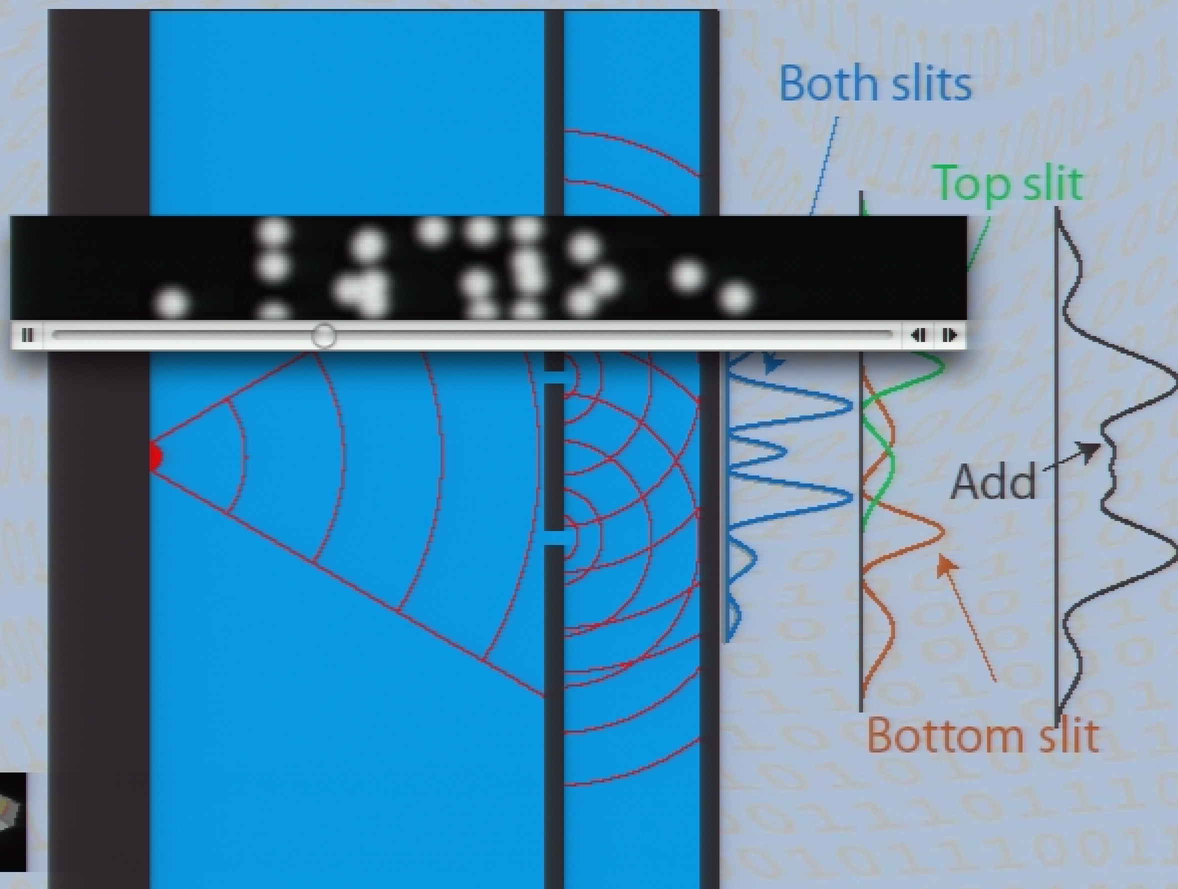
Basics of Quantum Mechanics

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.



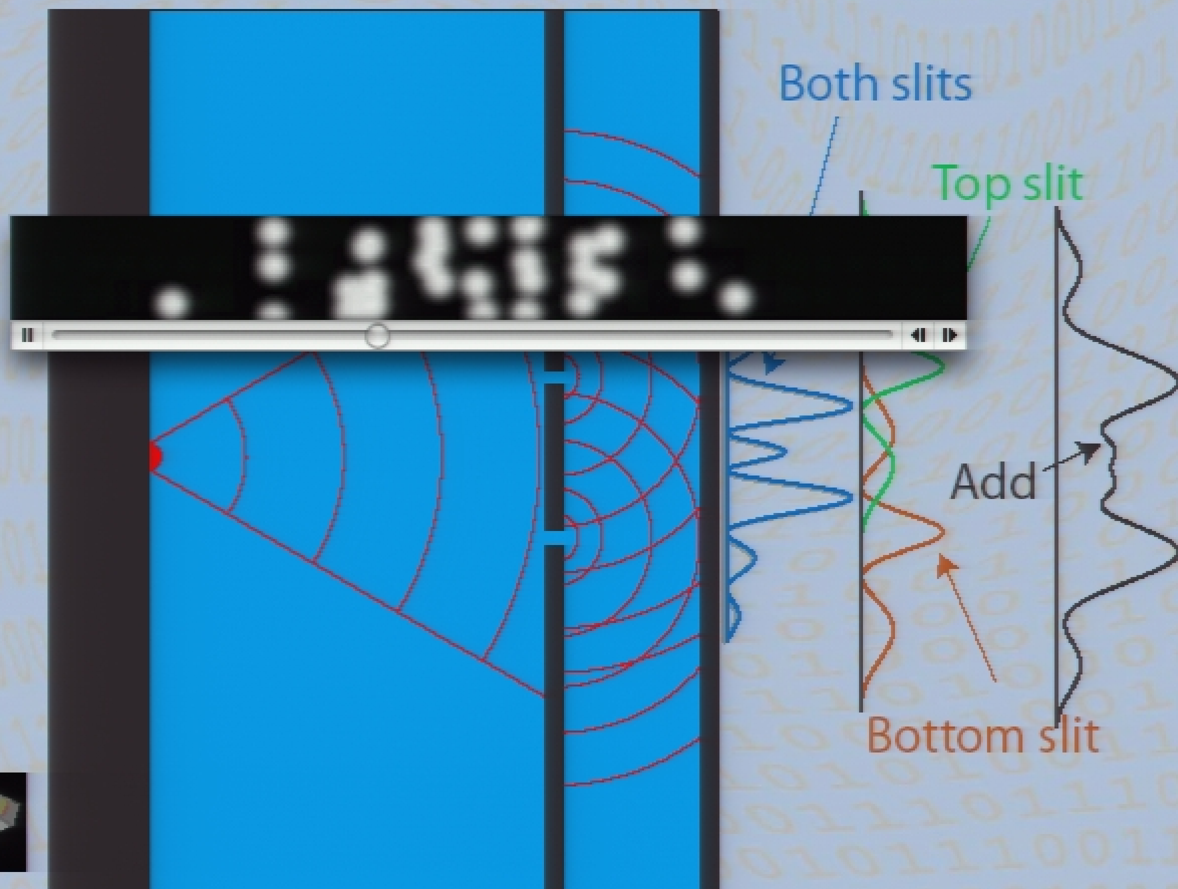
Basics of Quantum Mechanics

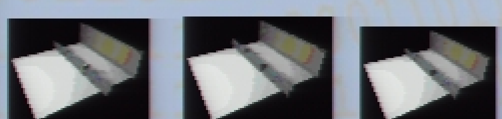
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.



Basics of Quantum Mechanics

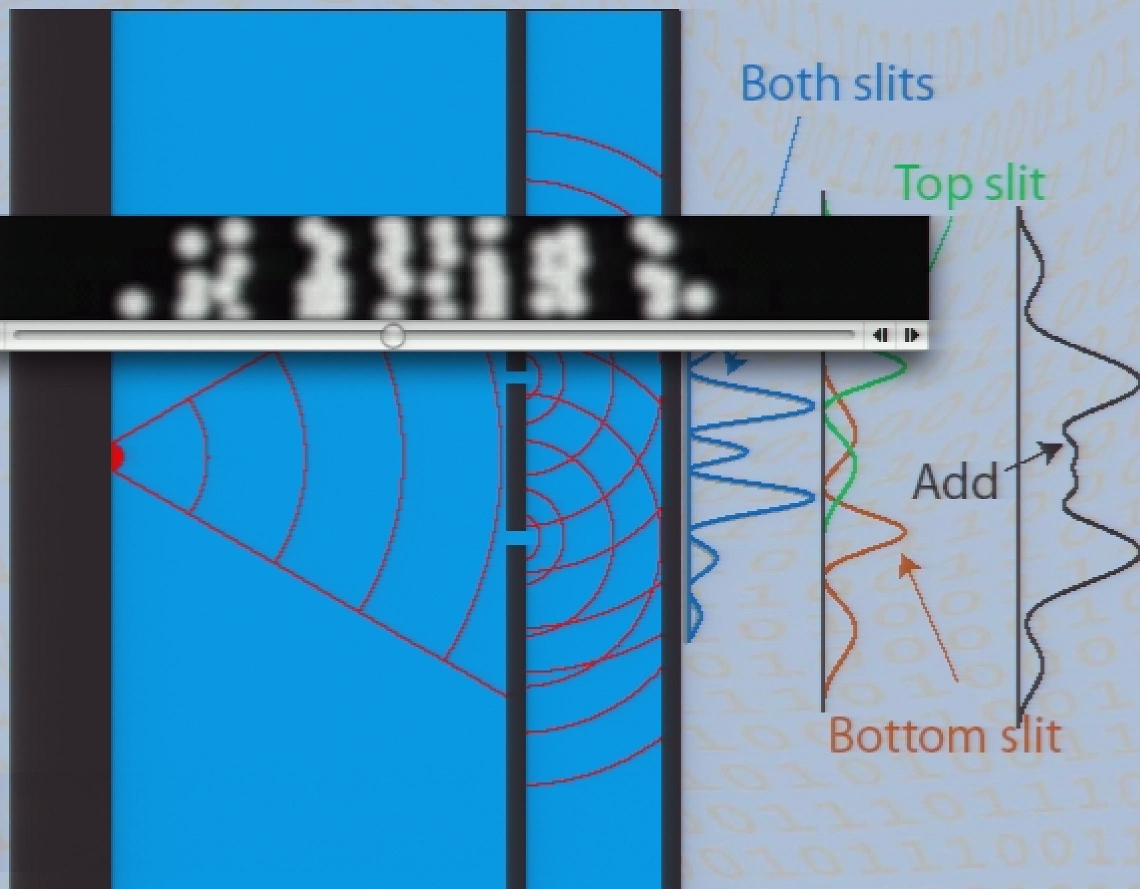
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

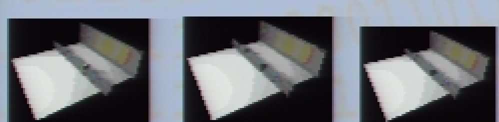




Basics of Quantum Mechanics

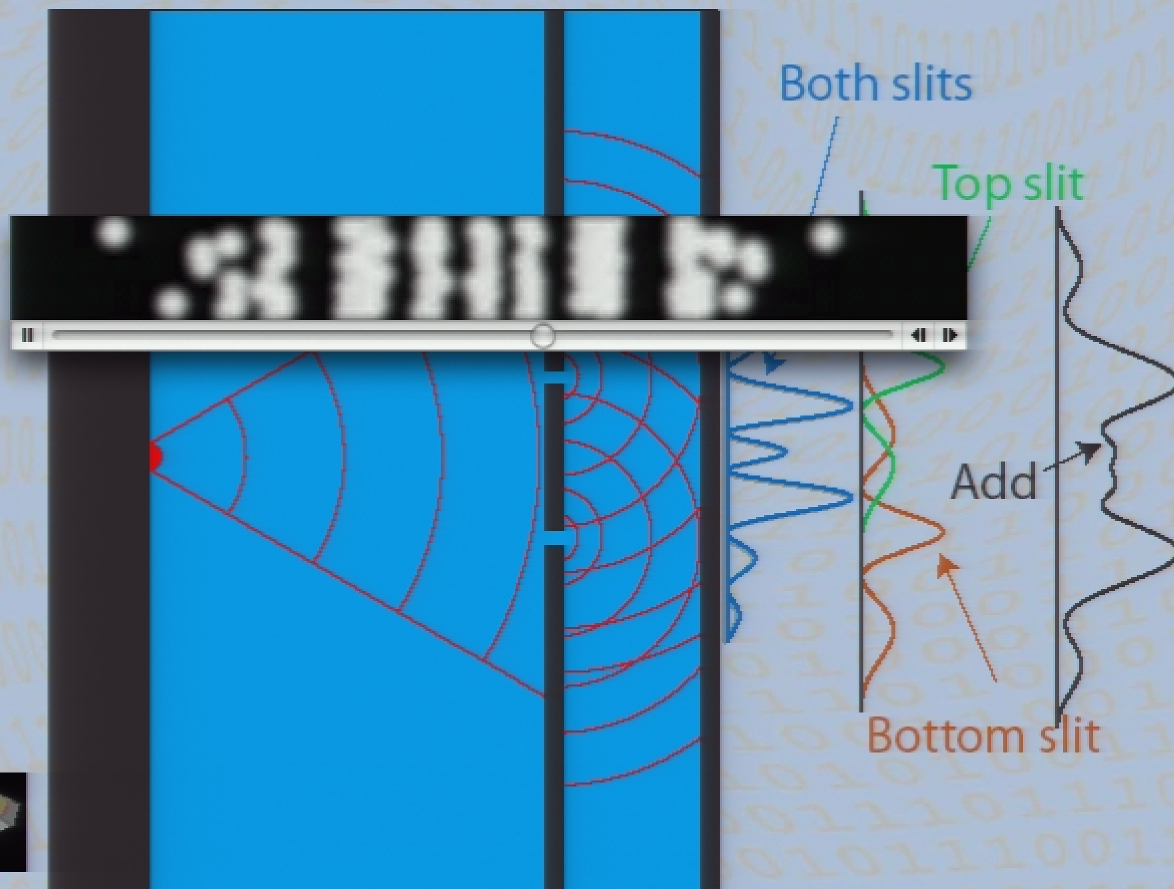
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

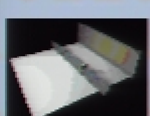


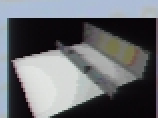


Basics of Quantum Mechanics

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.

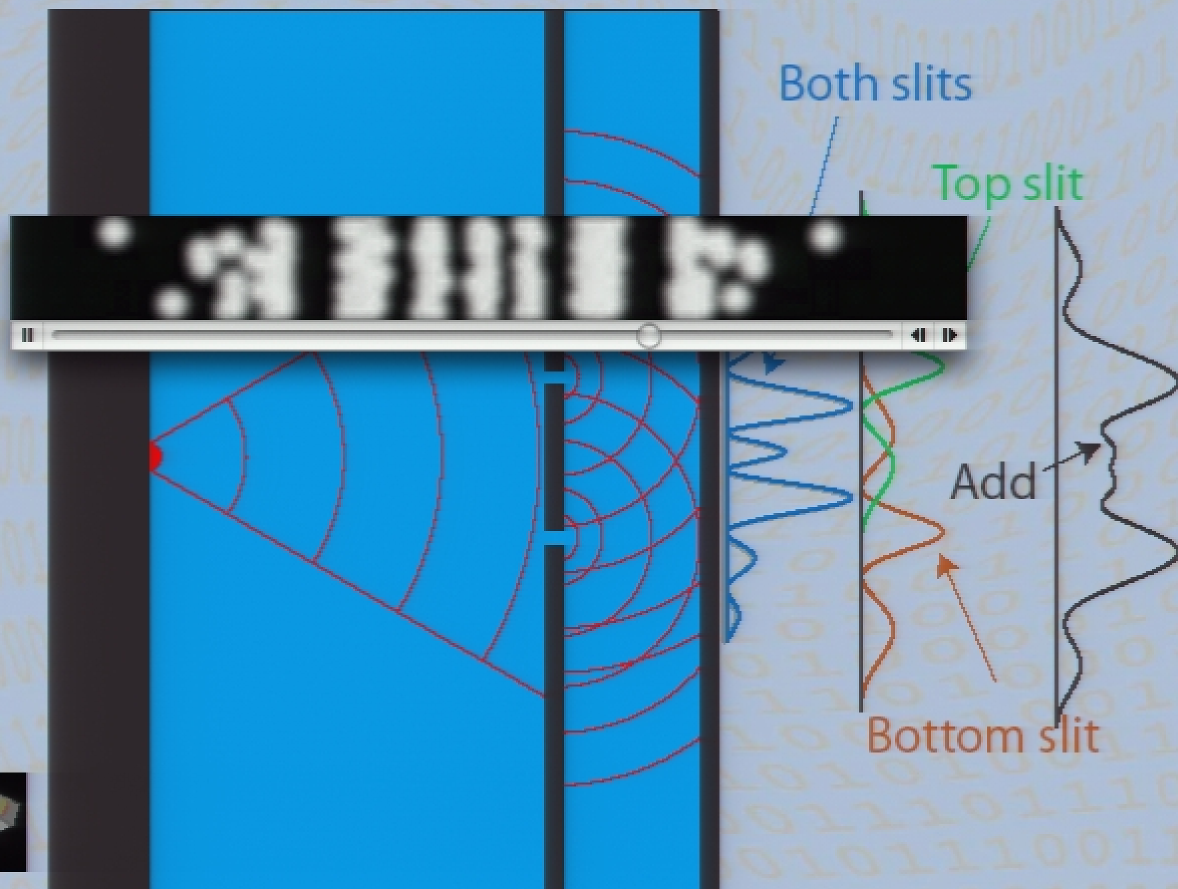


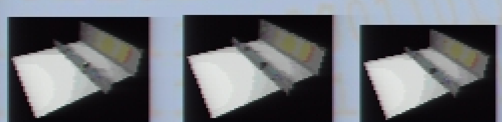




Basics of Quantum Mechanics

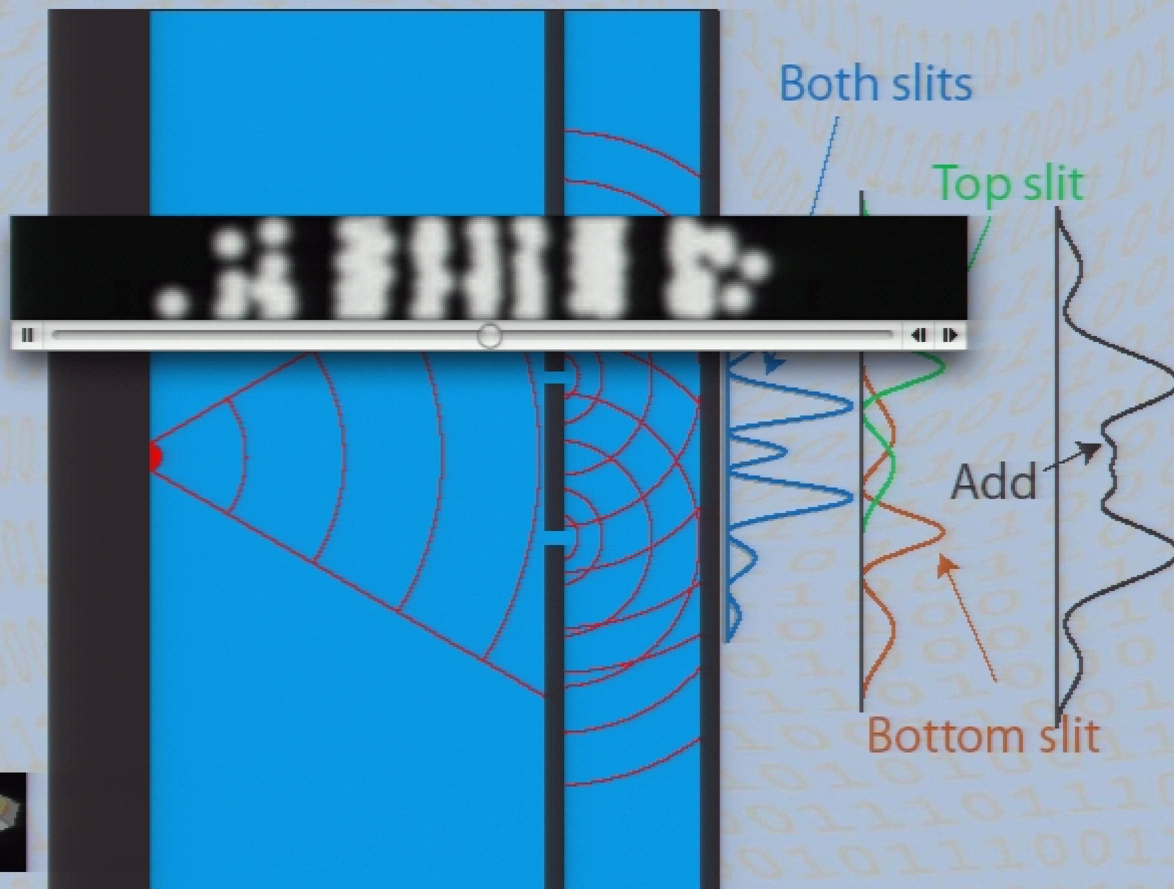
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

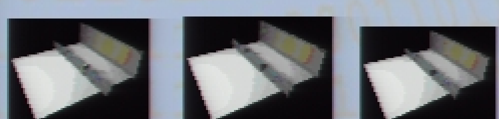




Basics of Quantum Mechanics

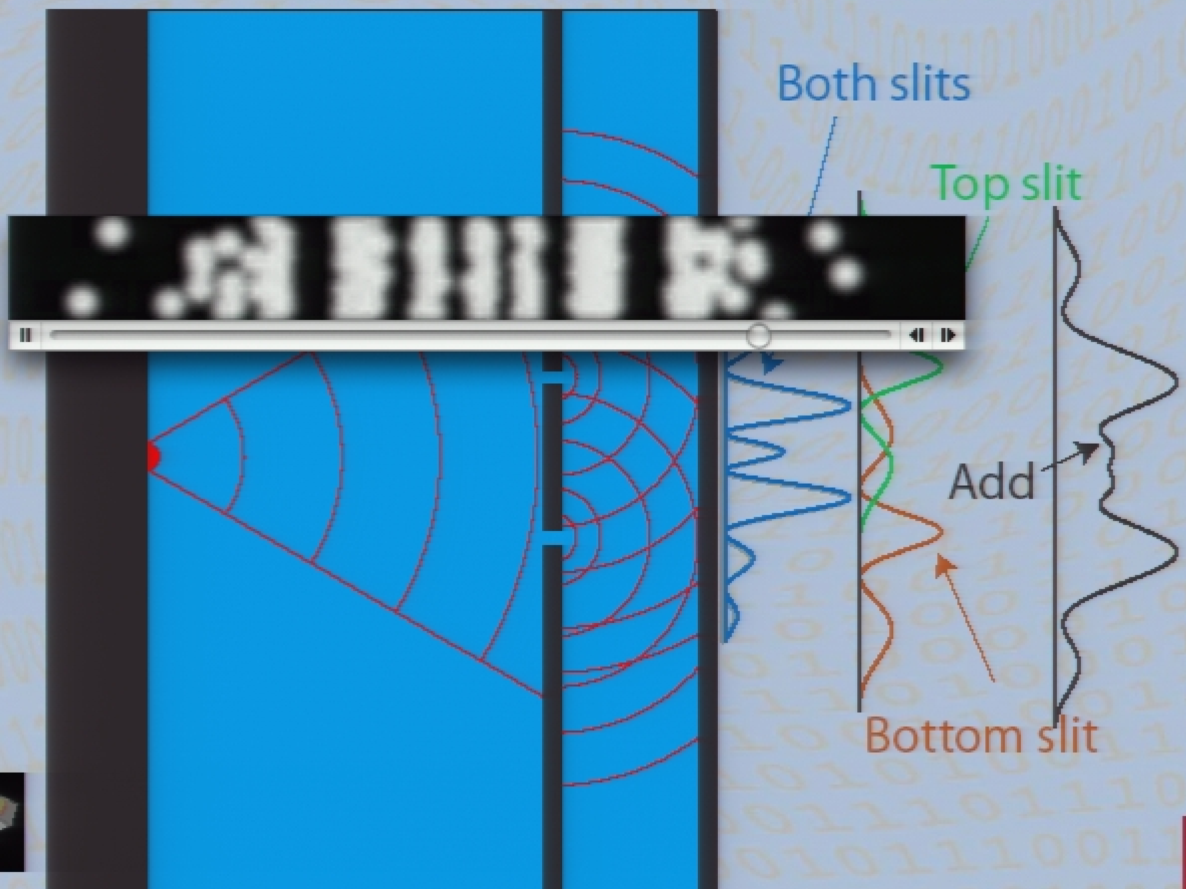
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

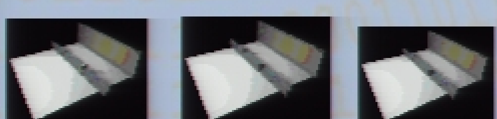




Basics of Quantum Mechanics

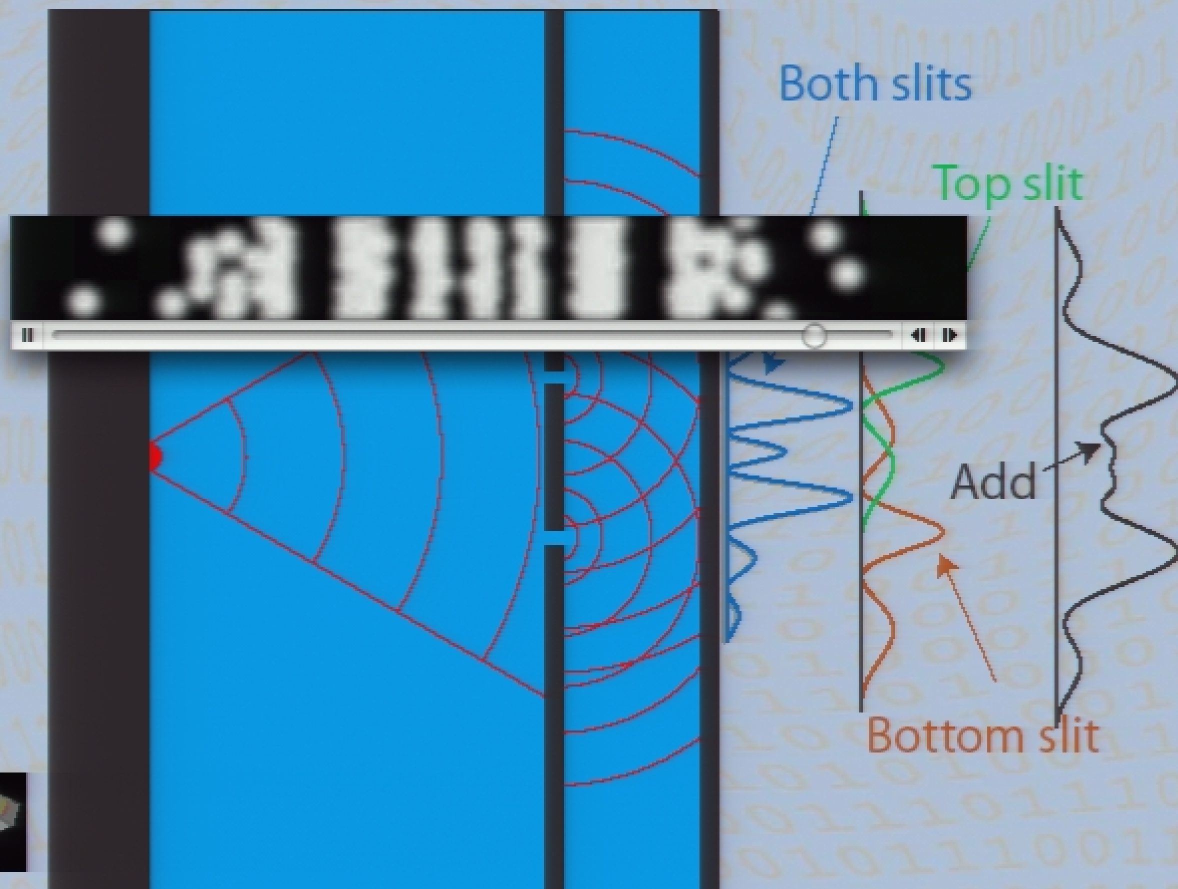
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.





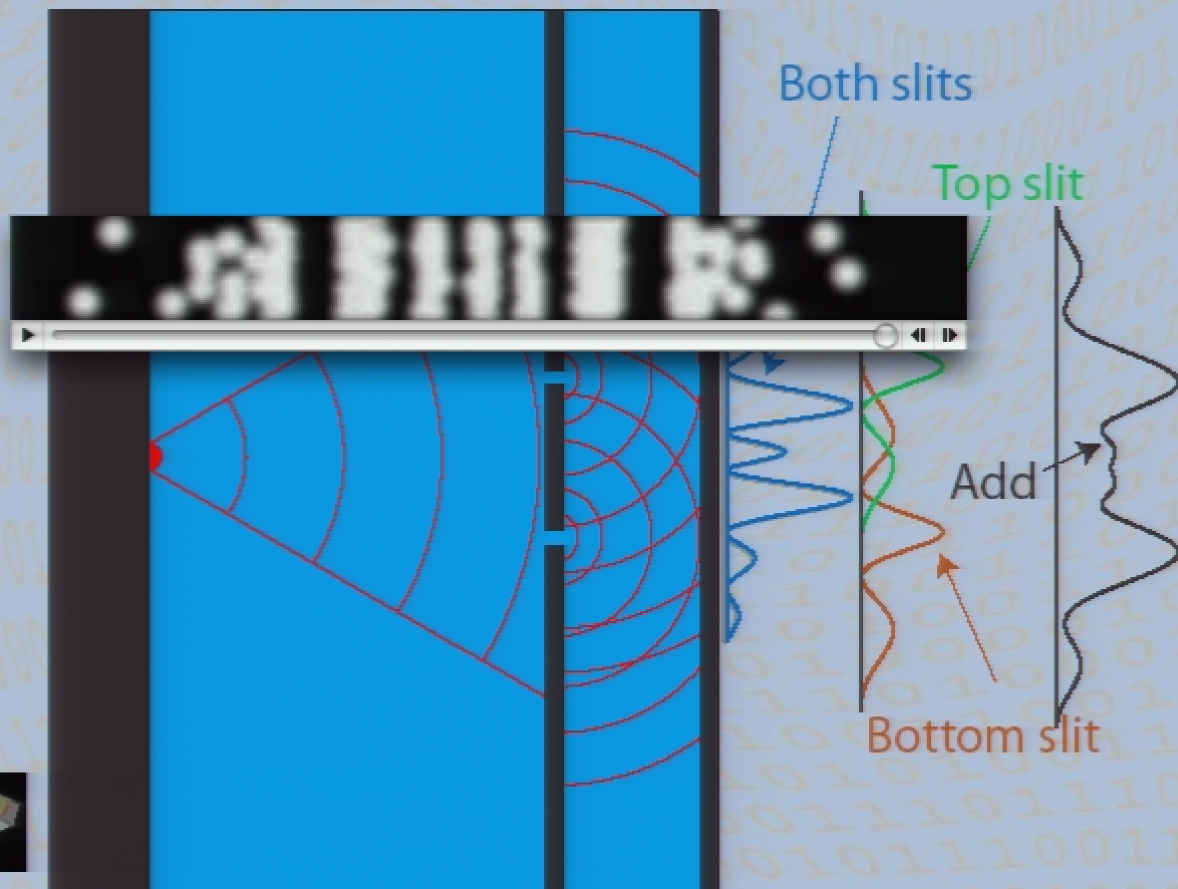
Basics of Quantum Mechanics

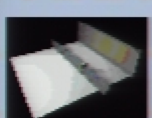
A coherent light source such as a laser is shined through 2 slits, the result of each independent slit do not add up to the final result when both slits are open due to interference effects.

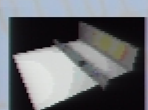


Basics of Quantum Mechanics

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.

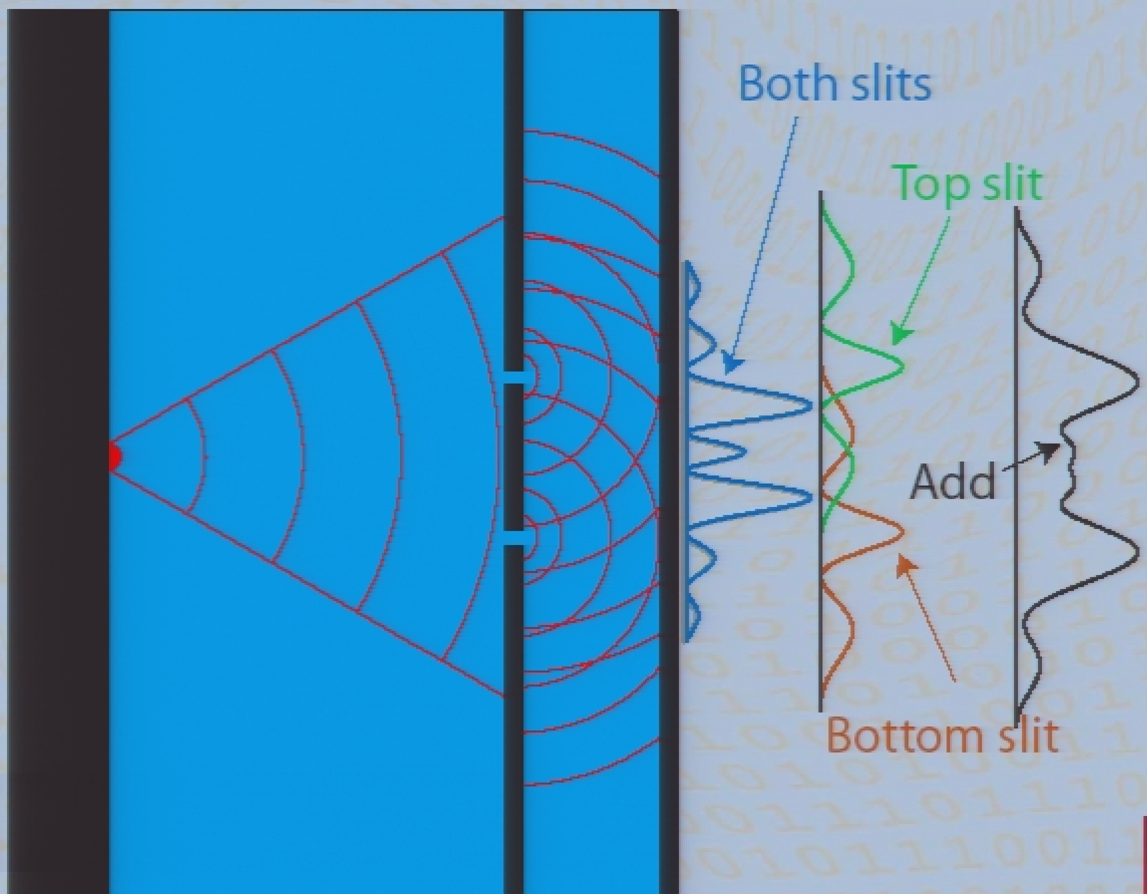






Basics of Quantum Mechanics

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.

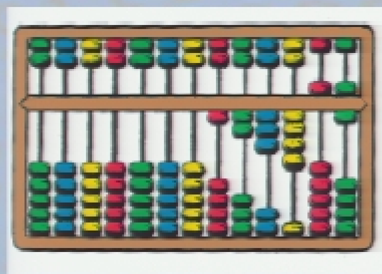


Two properties of Quantum Mechanics:

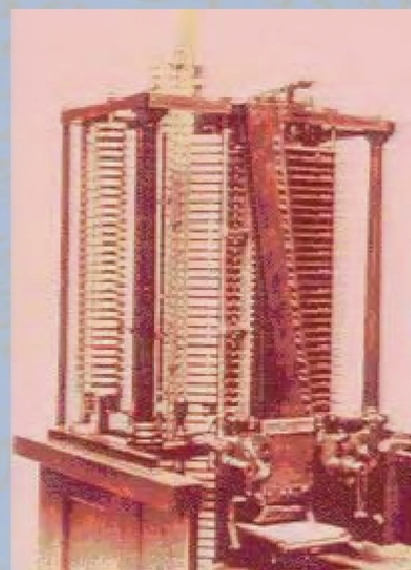
- Quantum systems behave both as waves and particles. These particles can be at more than one place at once.

- Looking at quantum systems always leaves a fingerprint.

Early computing devices



Abacus



Babbage
Analytical engine

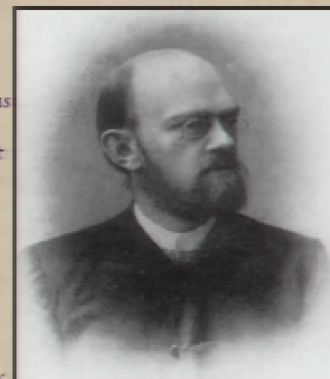
MIT's mechanical mind

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.

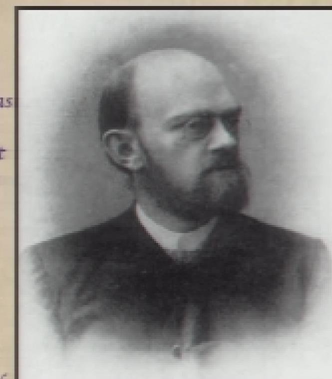
On the other hand a direct method is needed for the proof of the compatibility of the arithmetical axioms. The axioms of arithmetic are essentially nothing else than the known rules of calculation, with the addition of the axiom of continuity. I recently collected them4 and in so doing replaced the axiom 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 -l 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 them4 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

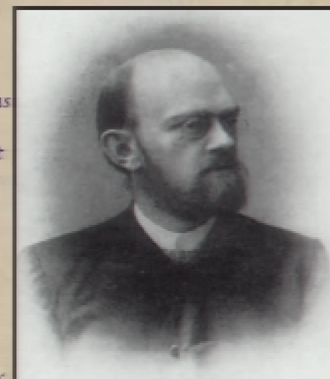
and intuition tell us. The concept of the continuum or even that of the system of all functions exists, then, in exactly the same sense as the system of integral, rational numbers, for example, or as Cantor's higher classes of numbers and cardinal numbers. For I am convinced that the existence of the 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.

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.

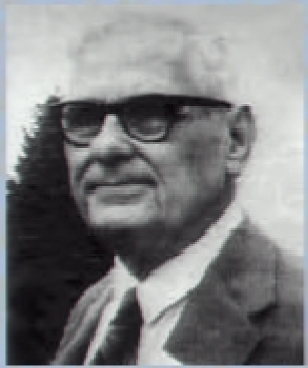
But above all I wish to designate the following as the most important among the numerous questions which can be asked with regard to the axioms: To prove that they are not contradictory, that is, that a definite number of logical steps based upon them can never lead to contradictory results.

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.

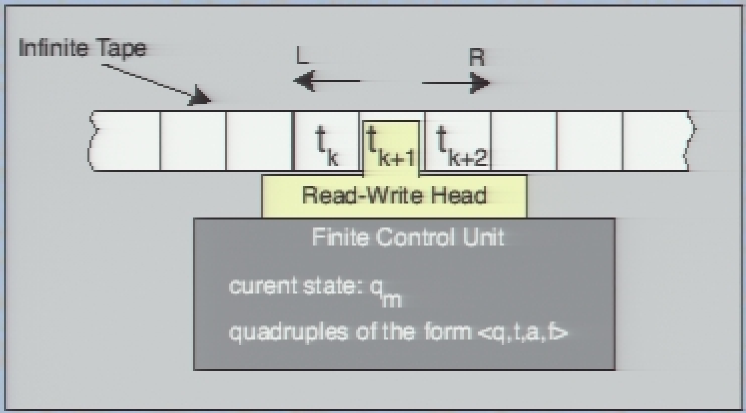
On the other hand a direct method is needed for the proof of the compatibility of the arithmetical axioms. The axioms of arithmetic are essentially nothing else than the known rules of calculation, with the addition of the axiom of continuity. I recently collected them4 and in so doing replaced the axiom 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.

Turing machines


Church


Turing



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

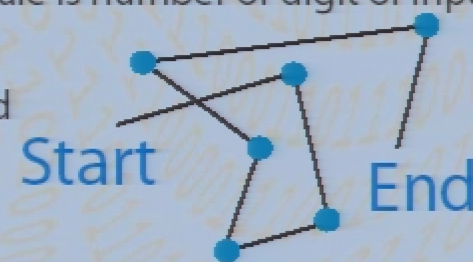
- Adding: 748230+3802=752032

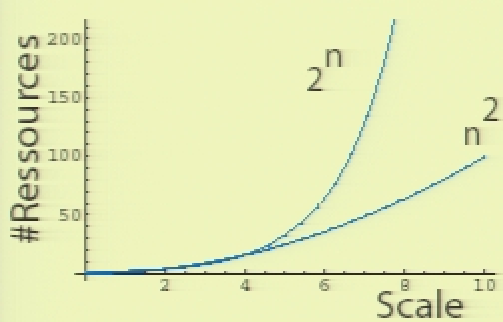
  Scale is number of digit of input
- Factor in product of primes: 54029=97x557

  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

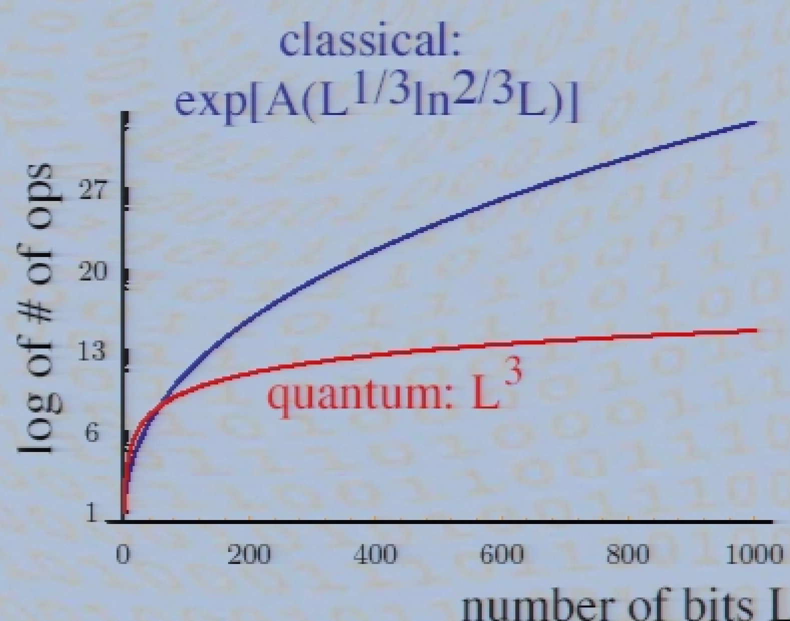
(Shor, IEEE Press 1994)

Peter Shor

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

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

Complexity theory

Goal: asses the amount of ressources to solve problems

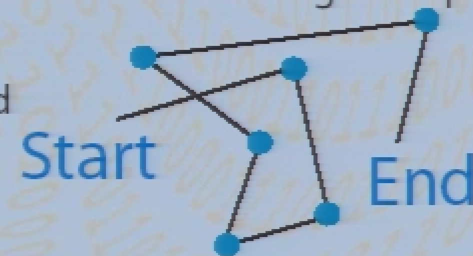
- Adding: 748230+3802=752032

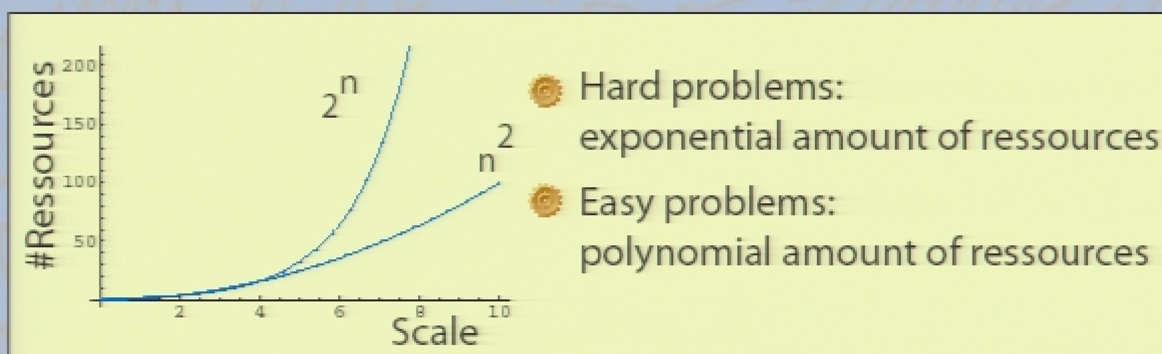
  Scale is number of digit of input
- Factor in product of primes: 54029=97x557

  Scale is number of digit of input
- Travelling salesperson:

  Find the shortest route from Start to End

  Scale is number of cities





Strong Church Turing principle:
no machine can turn a hard problem into an easy one

Quantum Factoring

Peter Shor

(Shor, IEEE Press 1994)

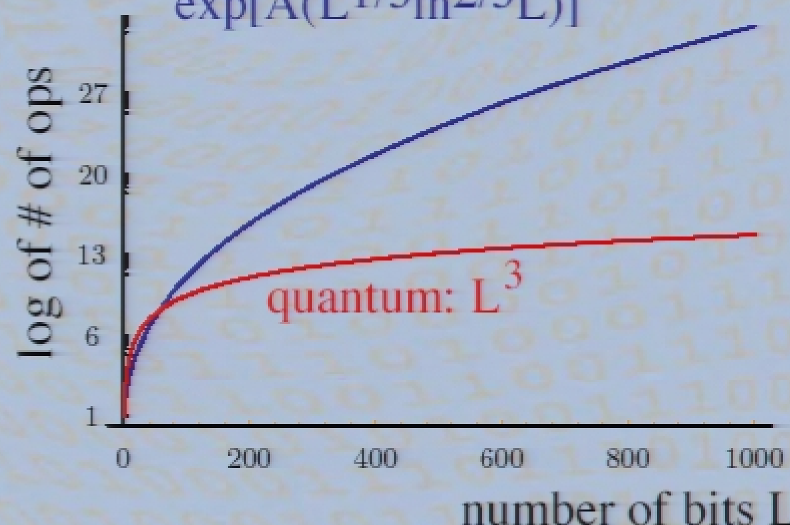
n=pq   (L = ln n)

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

Quantum algorithm

# of gates ~$12L^3$

# of qubits ~5L

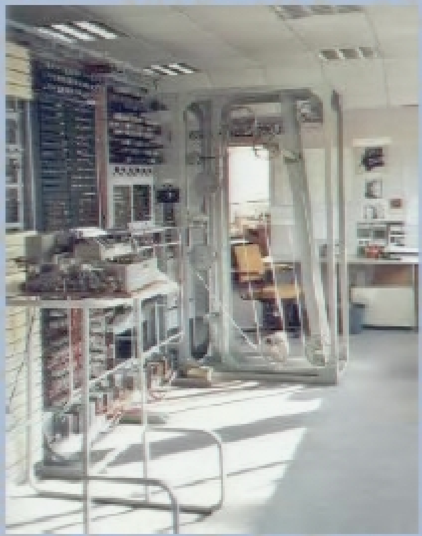


RSA Data Security.
A Security Dynamics Company

William T. Tutte

Centre for Applied Cryptographic Research — The University of Waterloo

Colossus,the first electronic computer,
was used to break FISH



Distinguished Professor Emeritus at UW

The difficulty of simulating a Quantum Computer

=

evaluating a Tutte polynomial

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 → 0 or 0 → 1

And Gate

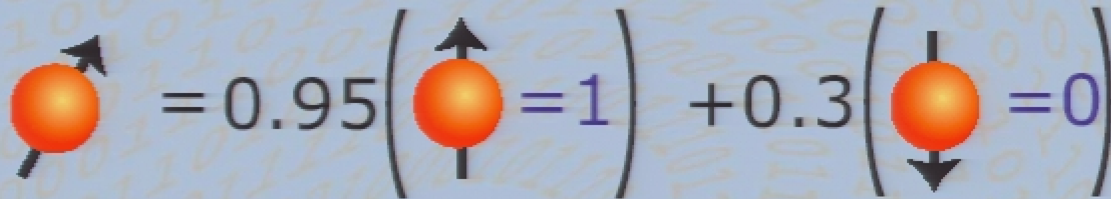
in		out
0	0	0
1	0	0
0	1	0
1	1	1

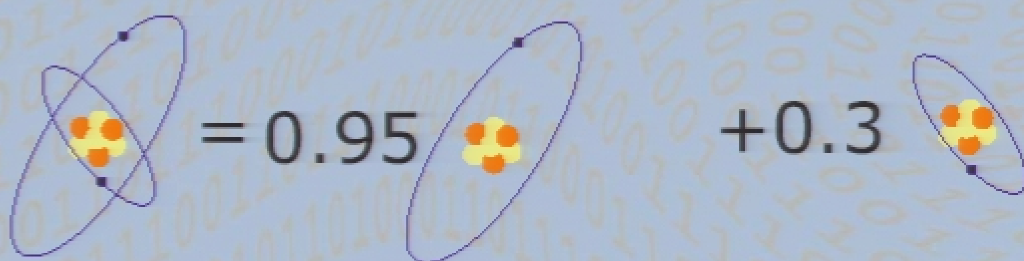
Input 1
Input 2 → Ouput

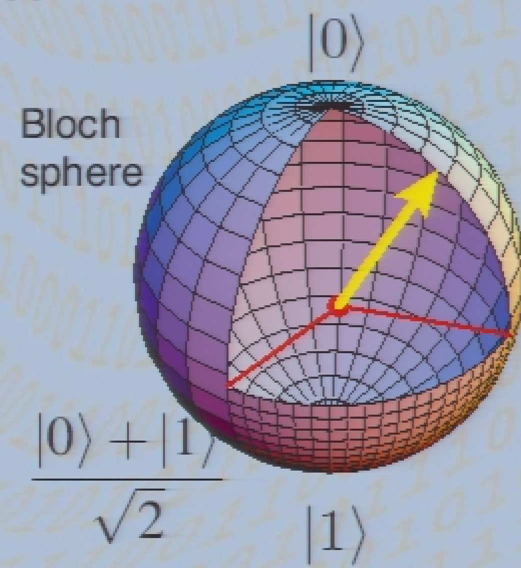
Input 1 And Input 2

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	$2^4=16$
⋮		⋮
10	0000000000,...	$2^{10}=1k$
20	0000000000...,	$2^{20}=1M$
30	0000000000...,	$2^{30}=1G$
40	0000000000...,	$2^{40}=1T$
50	0000000000...,	$2^{50}=1P$

The power of Quantum Computers

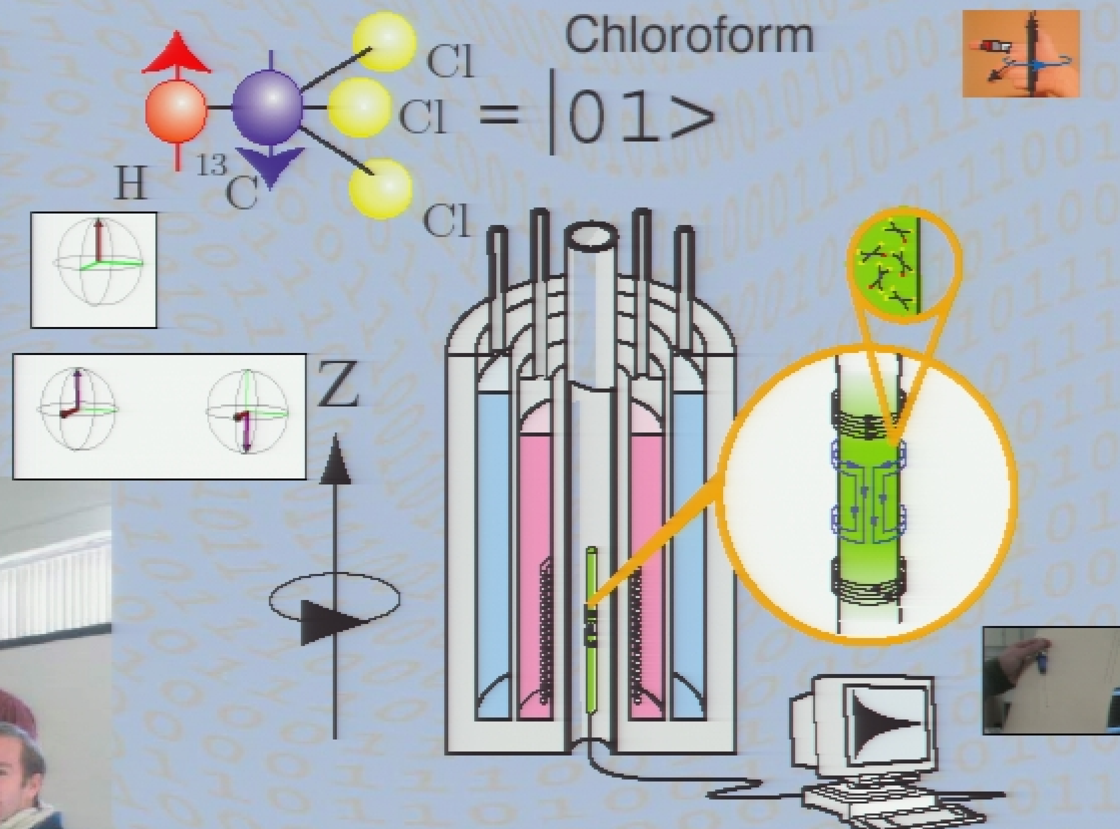
# of quantum bits	quantum states	# of classical bits
1	0,1	$2^1 = 2$
2	00,01,10,11	$2^2 = 4$
3	000,001,...,111	$2^3 = 8$
4	0000,0001,...,1111	$2^4 = 16$
⋮		⋮
10 ···	0000000000,...	$2^{10} = 1k$
20 ···	0000000000...,	$2^{20} = 1M$
30 ···	0000000000...,	$2^{30} = 1G$
40 ···	0000000000...,	$2^{40} = 1T$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

Theory vs experiment

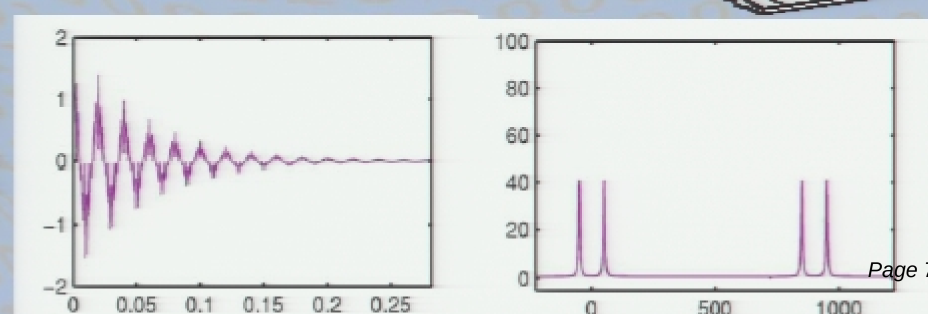
Nuclear Magnetic Resonance

Bloch

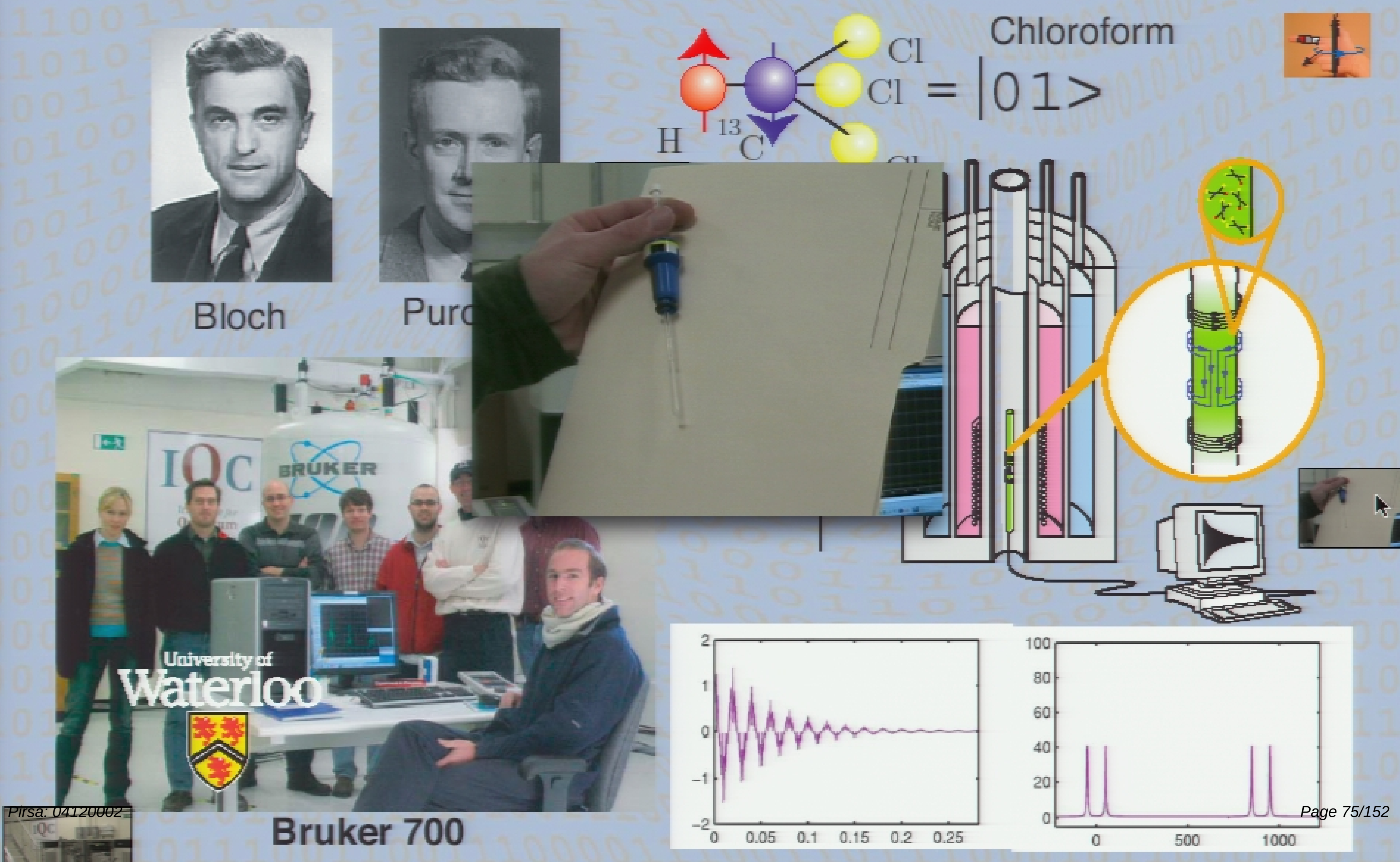
Purcell



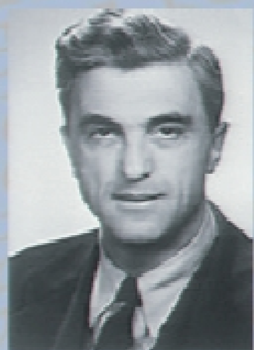
Bruker 700



Nuclear Magnetic Resonance

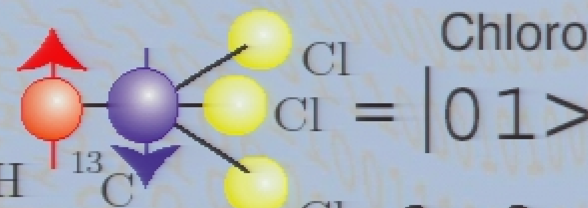


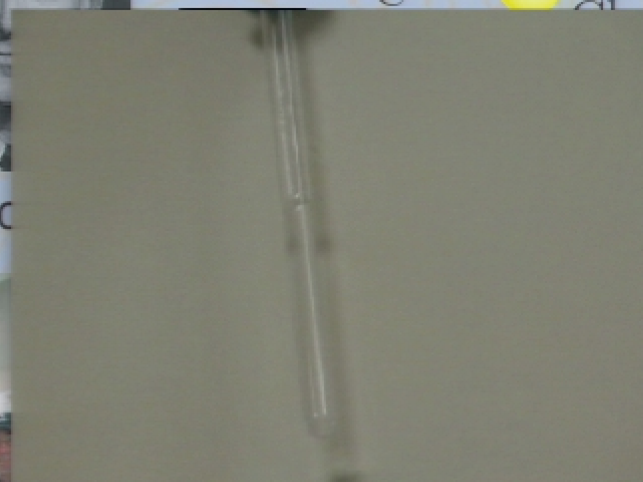
Nuclear Magnetic Resonance

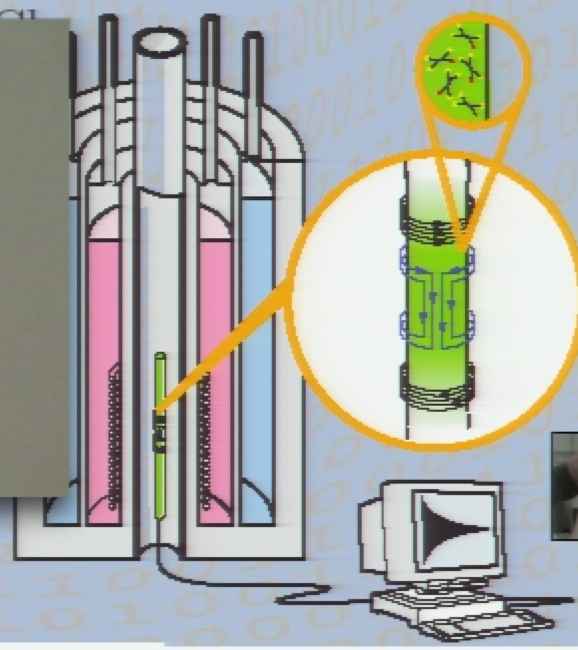


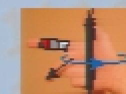
Bloch

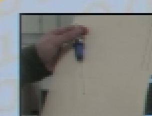
Purc



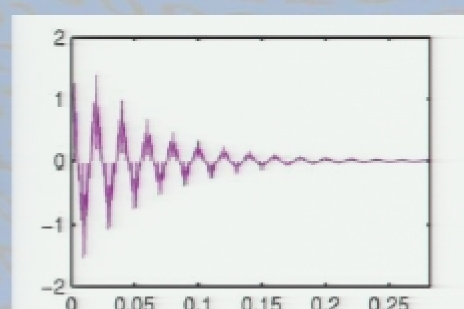


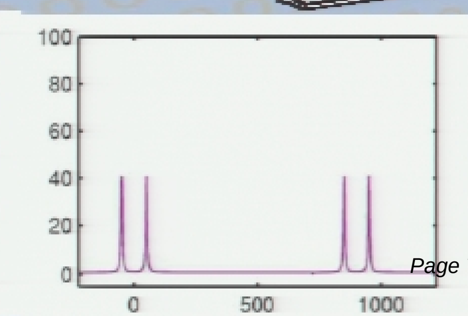


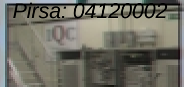




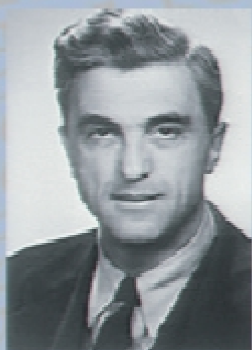
Bruker 700





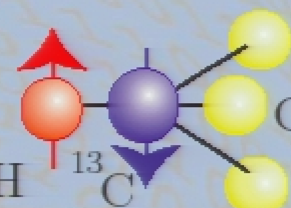


Nuclear Magnetic Resonance



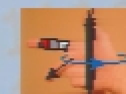
Bloch

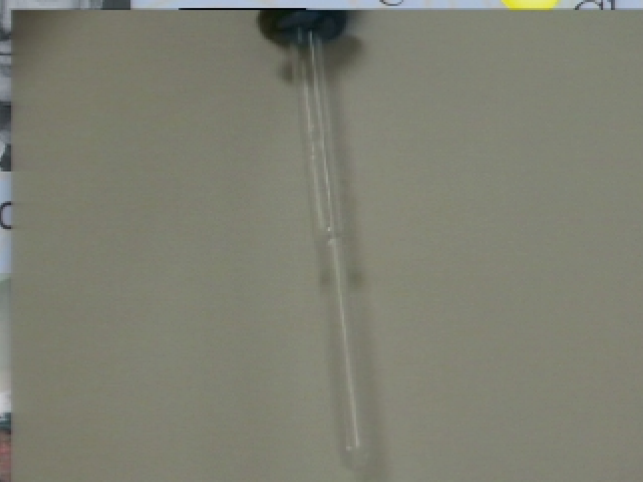
Purc

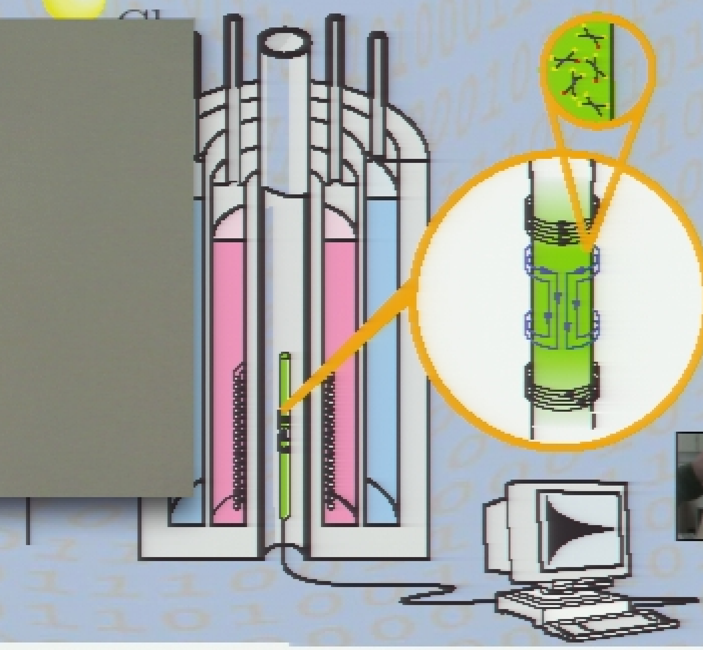


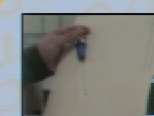
Chloroform

$= |01>$

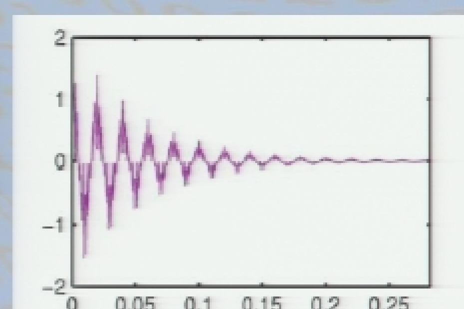


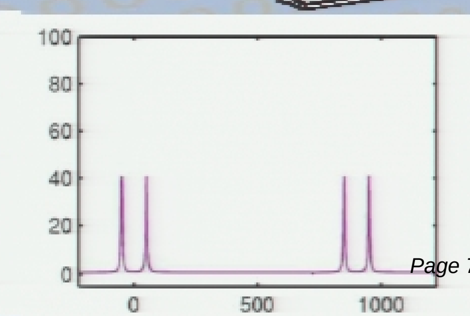


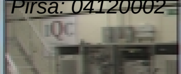




Bruker 700



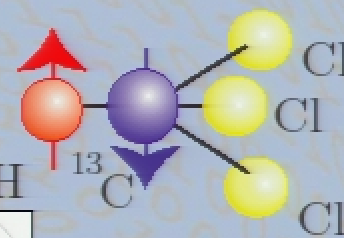




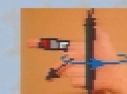
Nuclear Magnetic Resonance

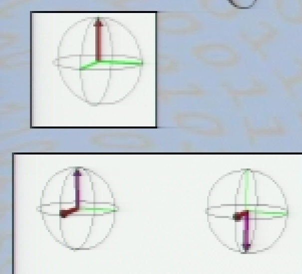
Bloch

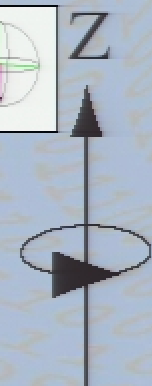
Purcell

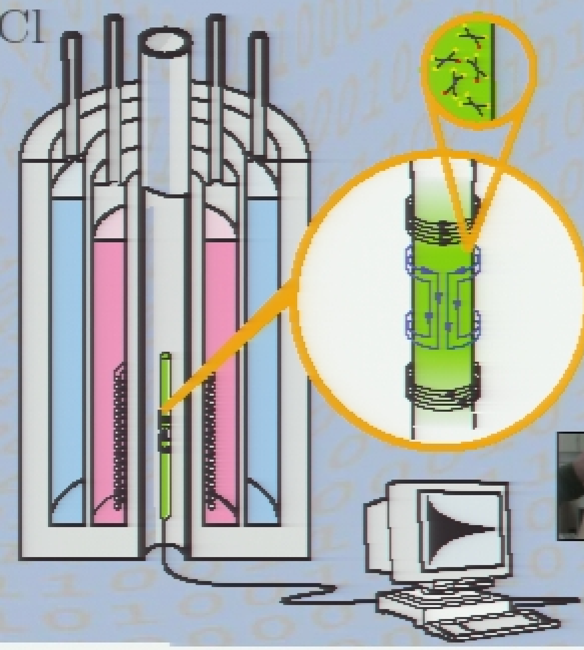


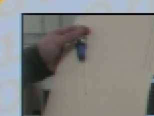
Chloroform $= |01>$



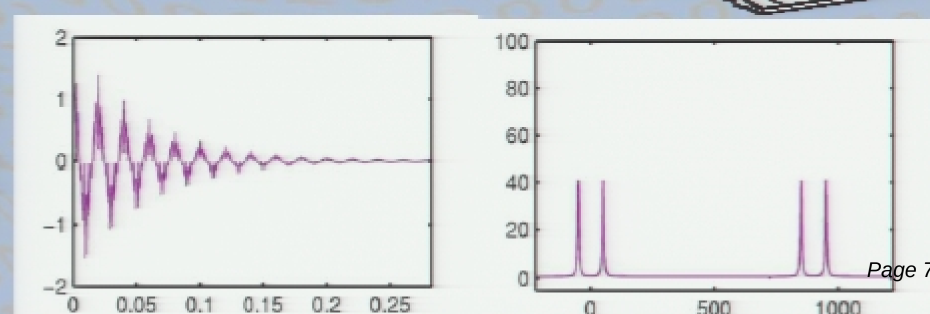


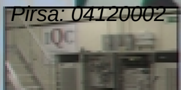




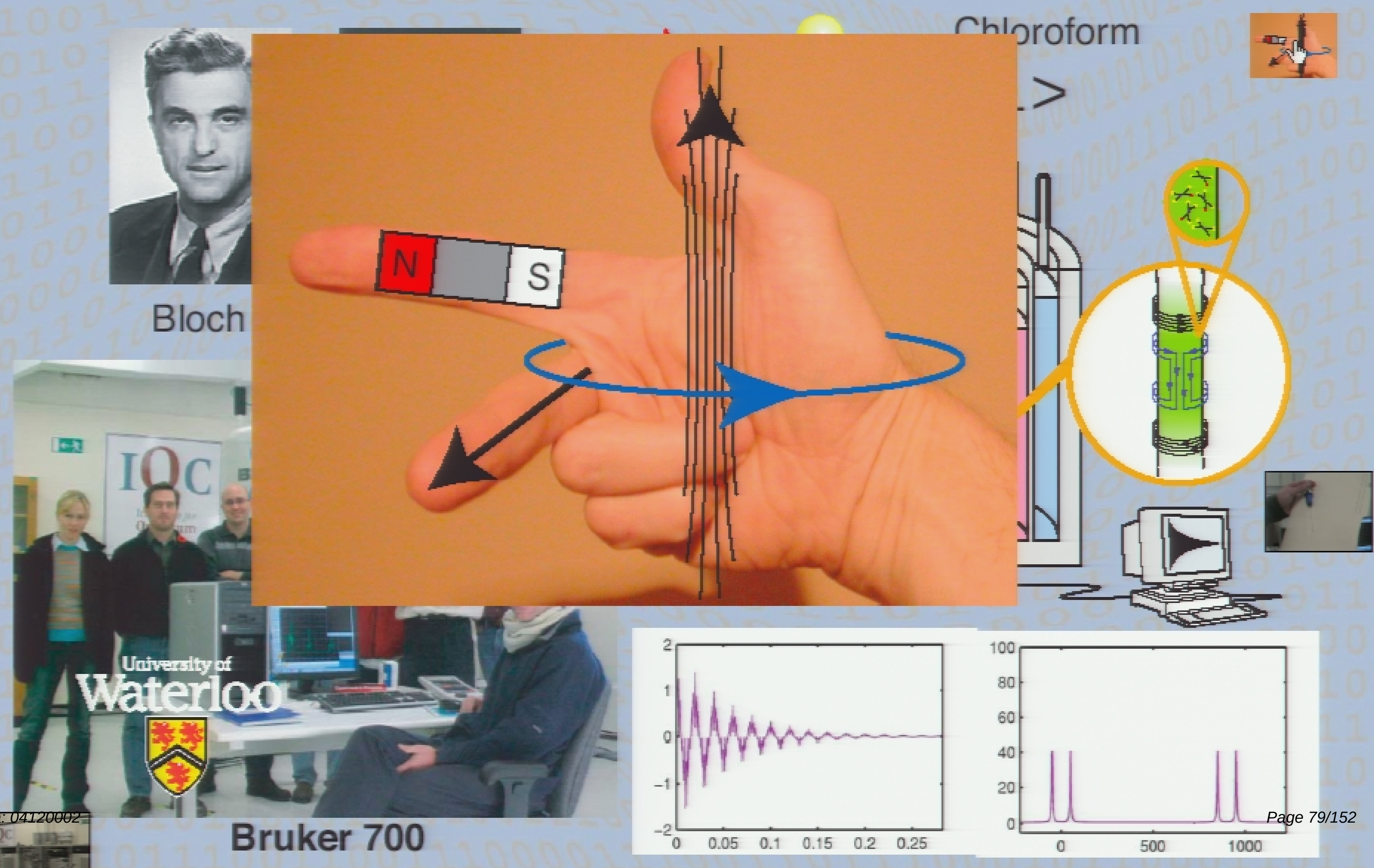


Bruker 700

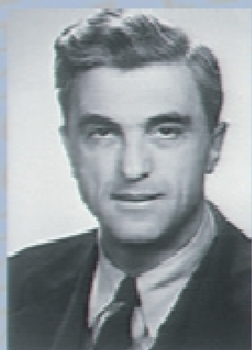




Nuclear Magnetic Resonance

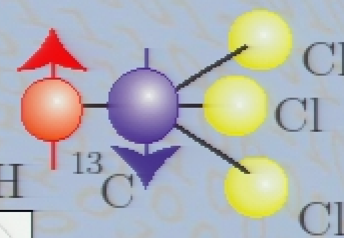


Nuclear Magnetic Resonance



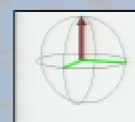
Bloch

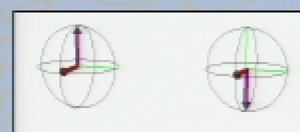
Purcell

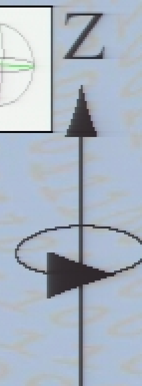


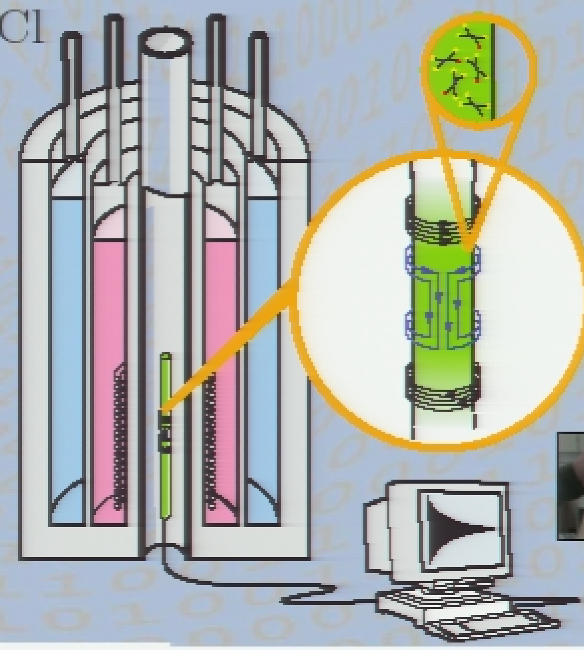
Chloroform

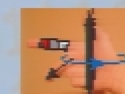
= |01>

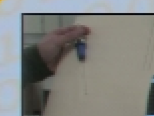




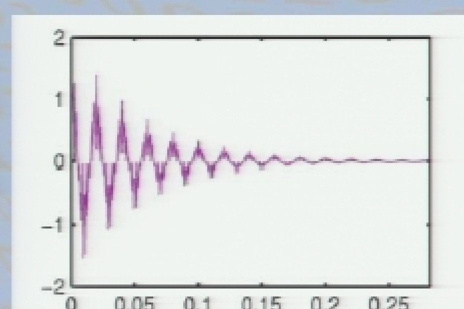


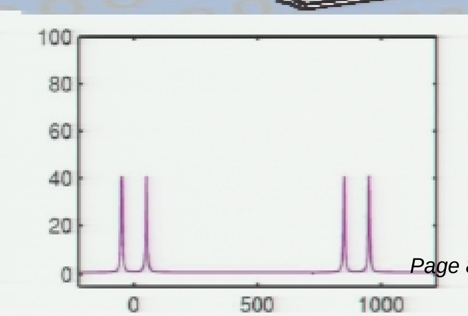


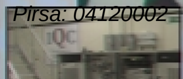




Bruker 700



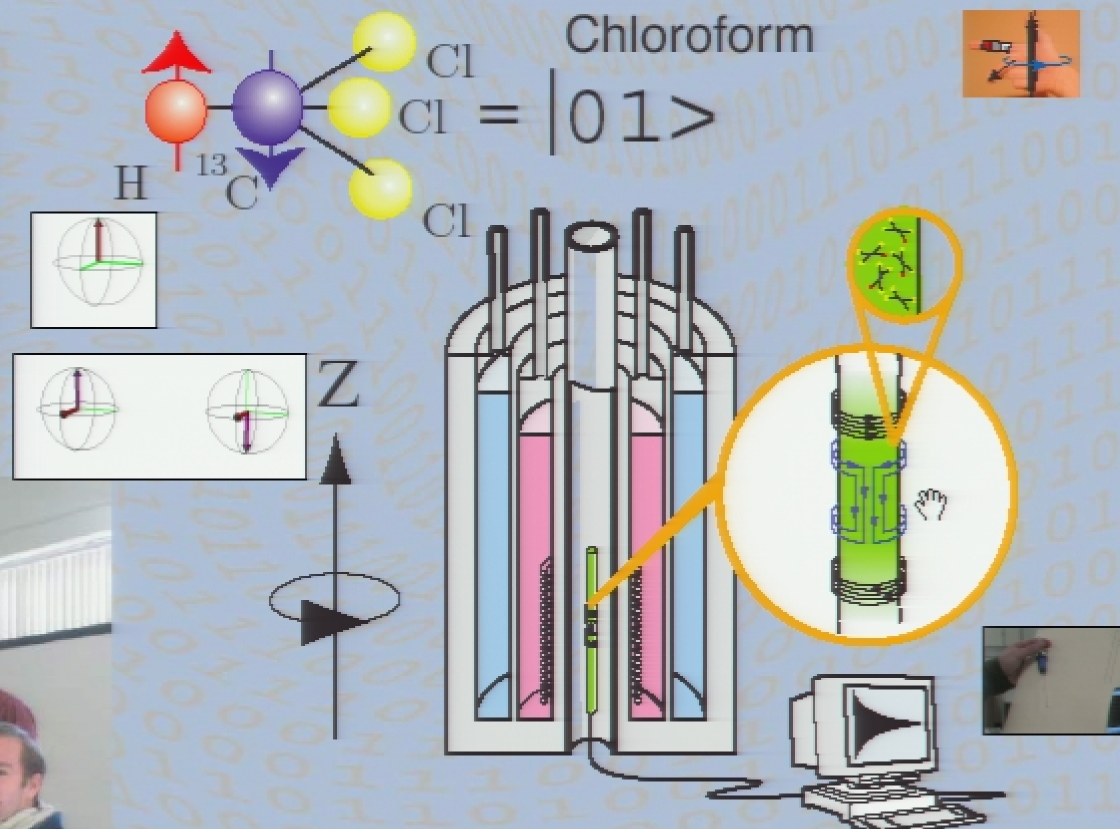




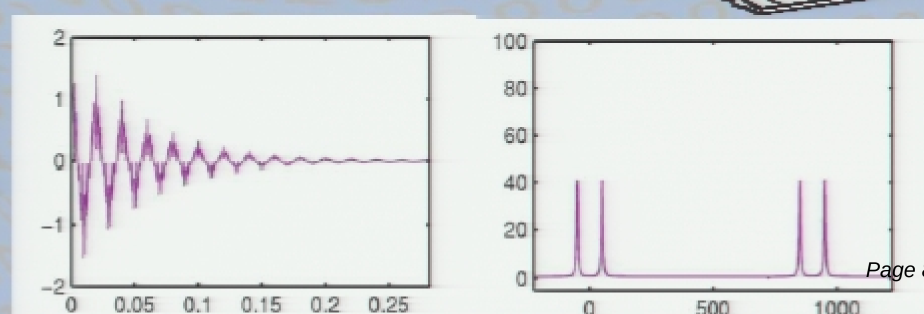
Nuclear Magnetic Resonance

Bloch

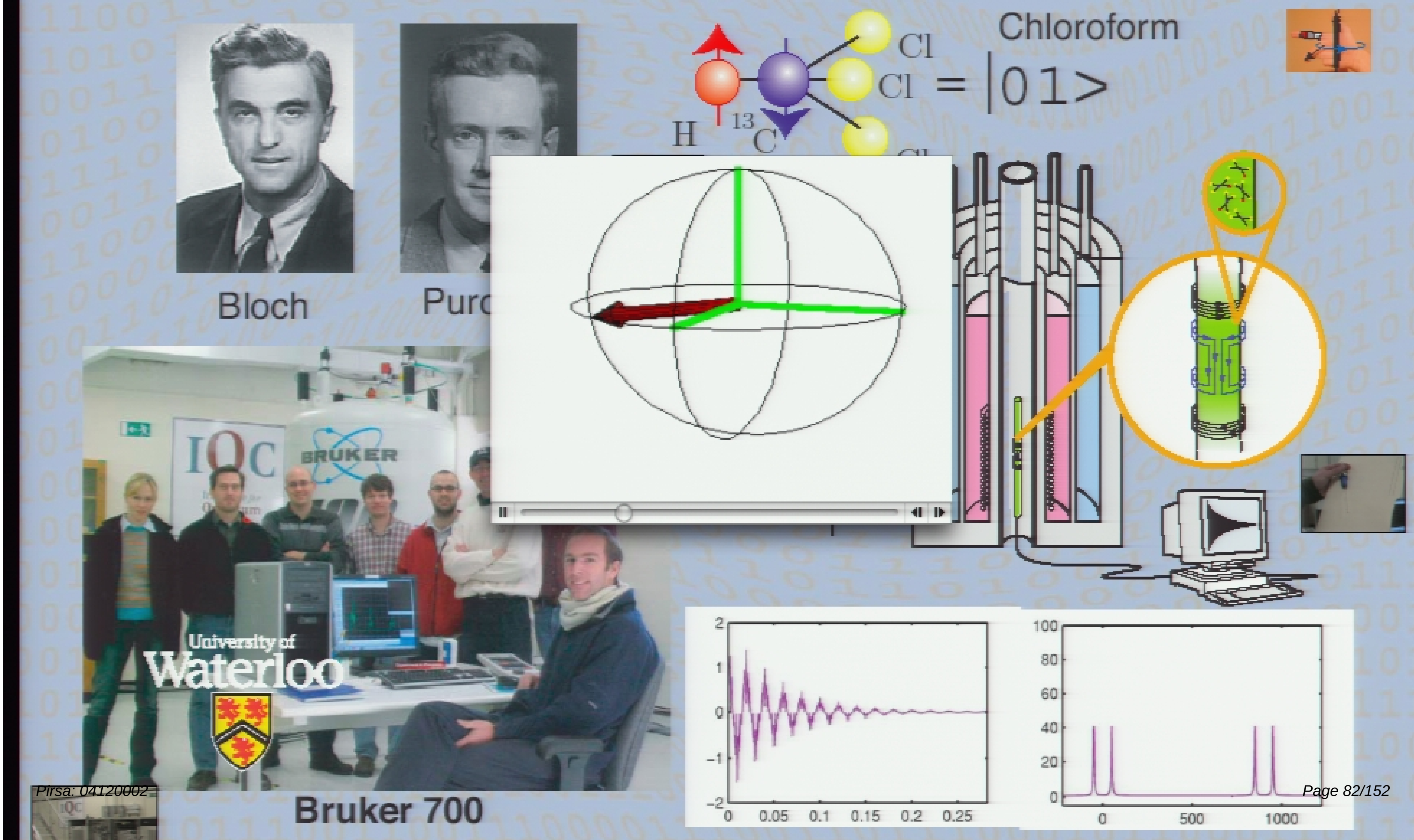
Purcell



Bruker 700



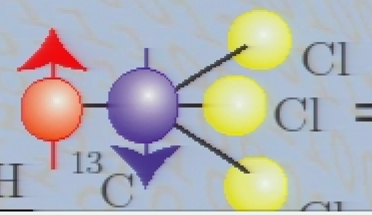
Nuclear Magnetic Resonance



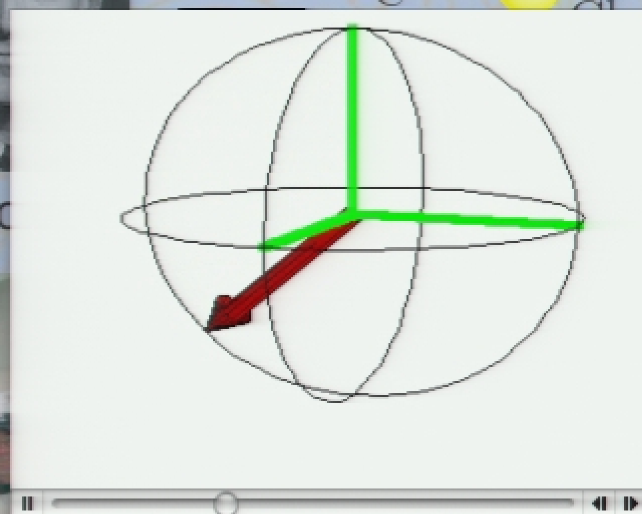
Nuclear Magnetic Resonance

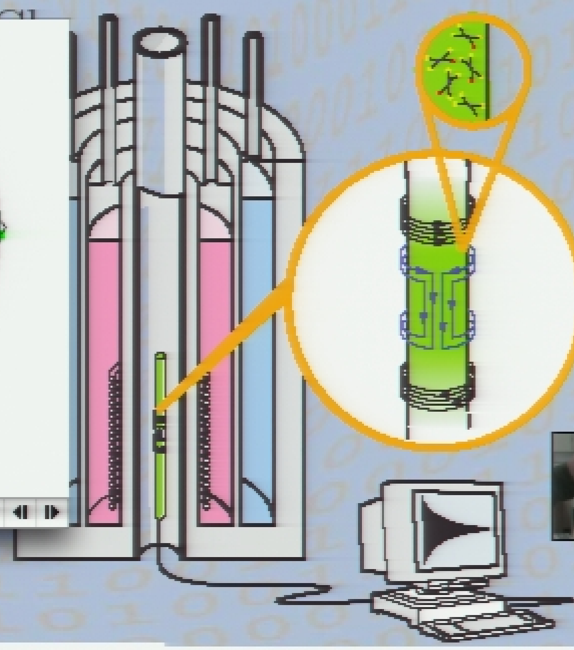
Bloch

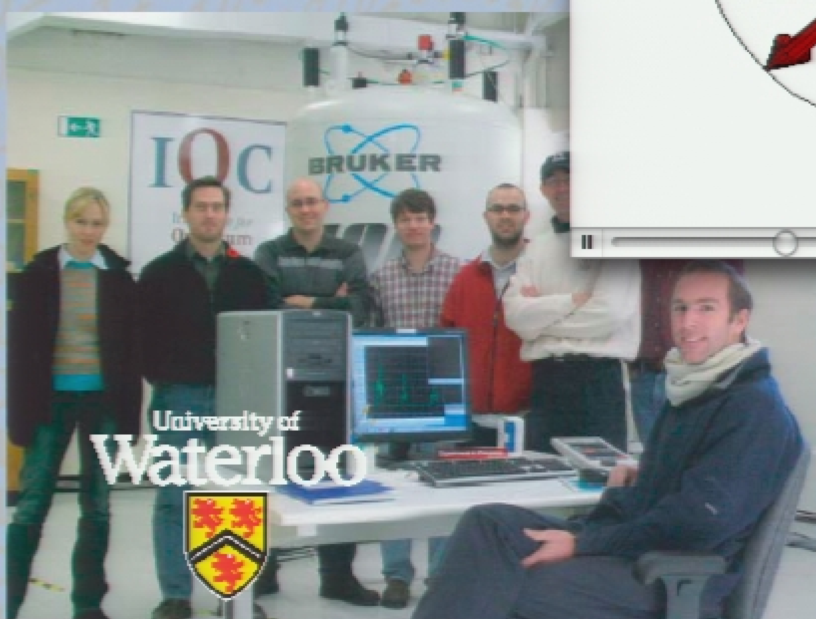
Purc



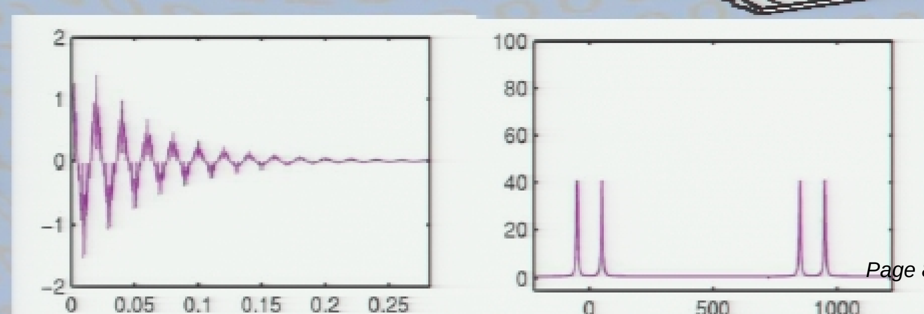
Chloroform $= |01\rangle$







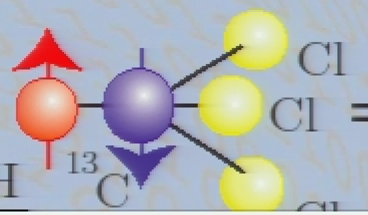
Bruker 700



Nuclear Magnetic Resonance

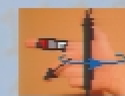
Bloch

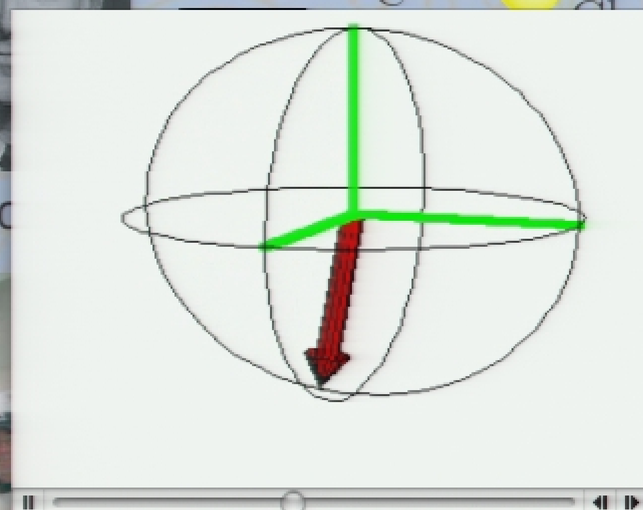
Purc

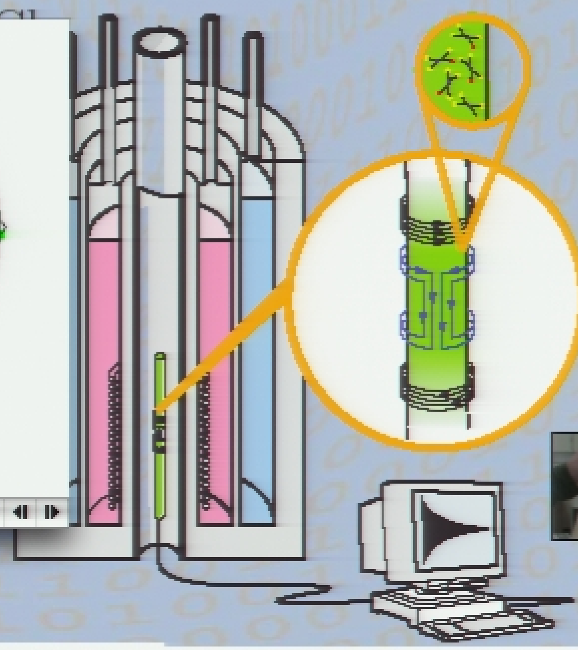


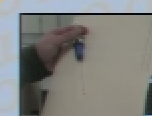
Chloroform

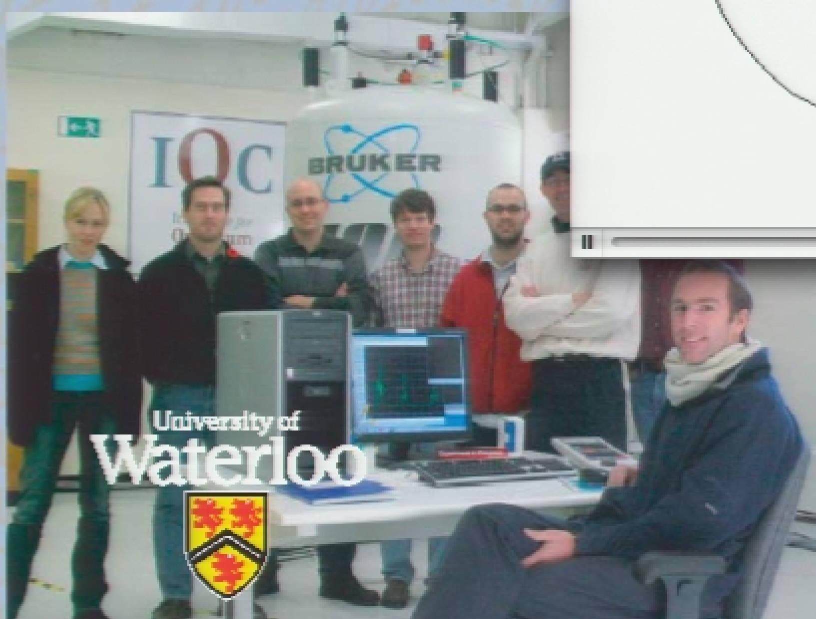
$= |01\rangle$



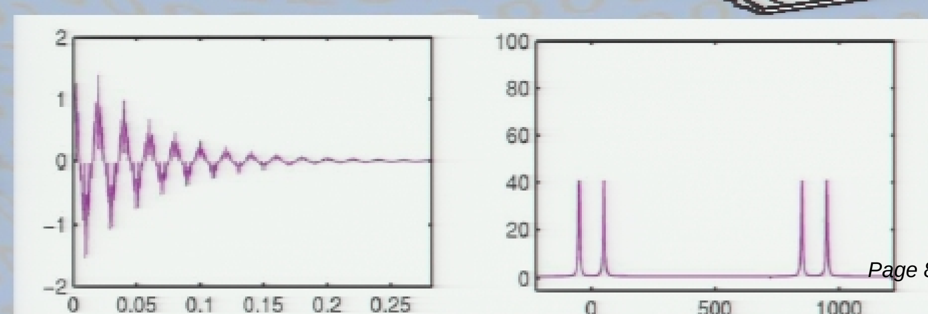


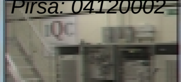




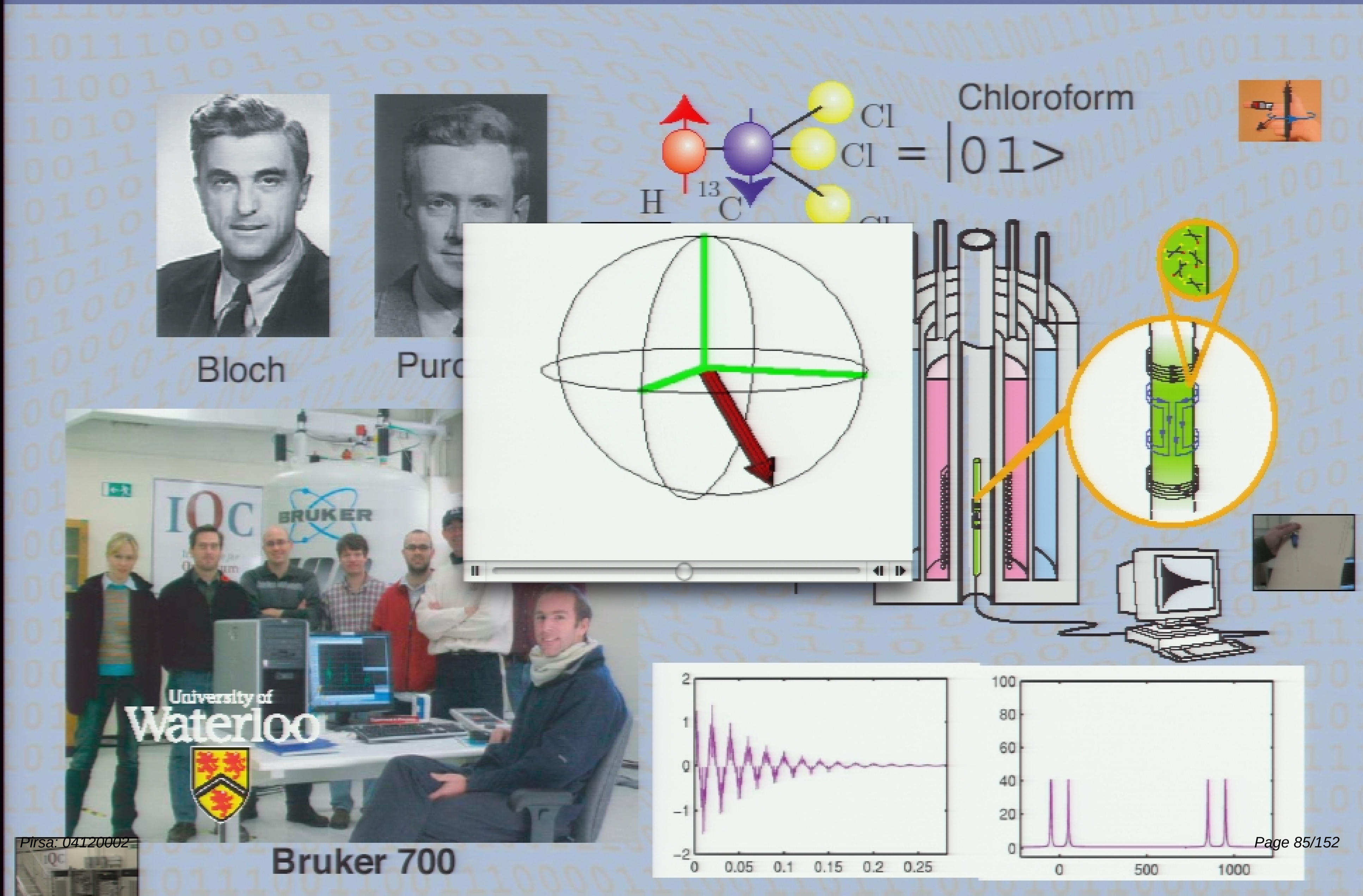


Bruker 700





Nuclear Magnetic Resonance

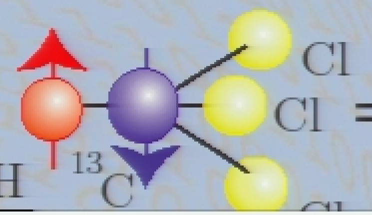


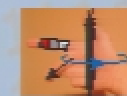
Nuclear Magnetic Resonance

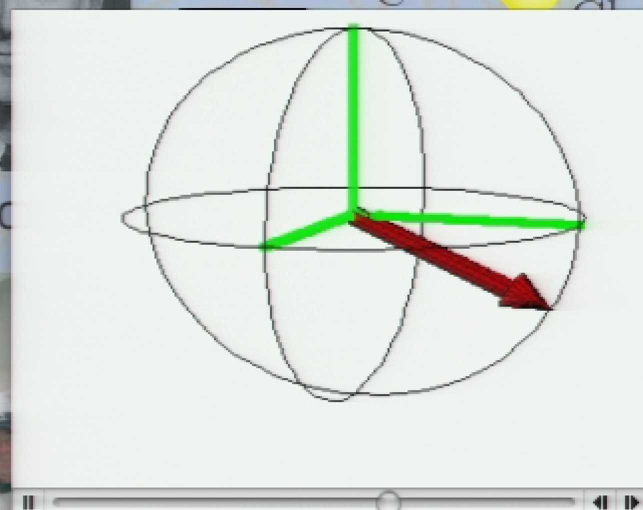
Bloch

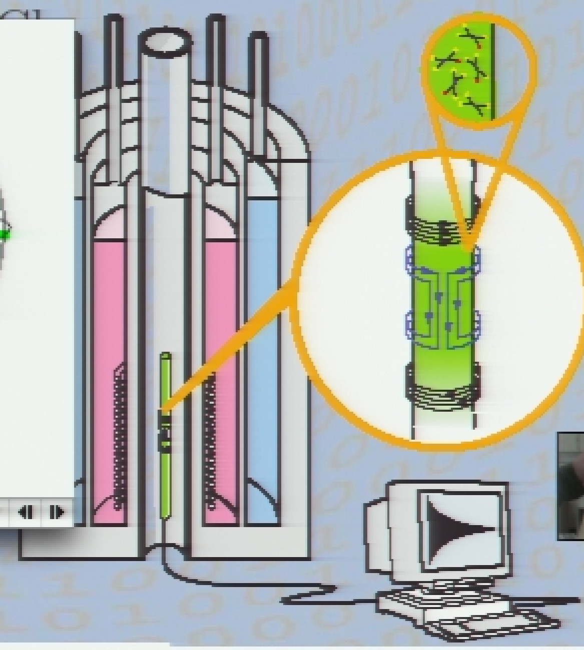
Purc

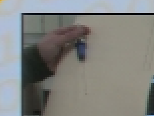
Chloroform

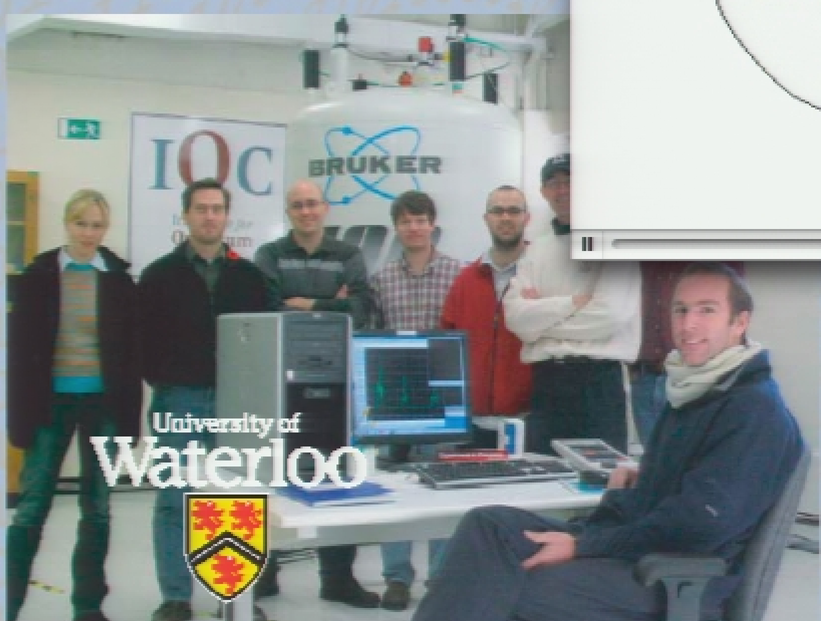




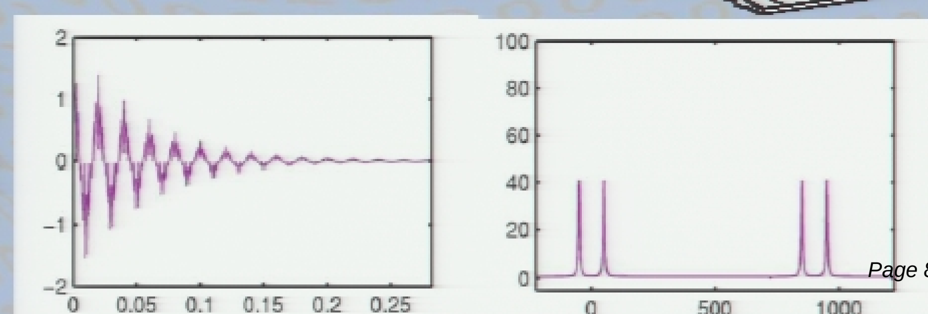


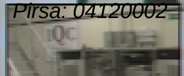




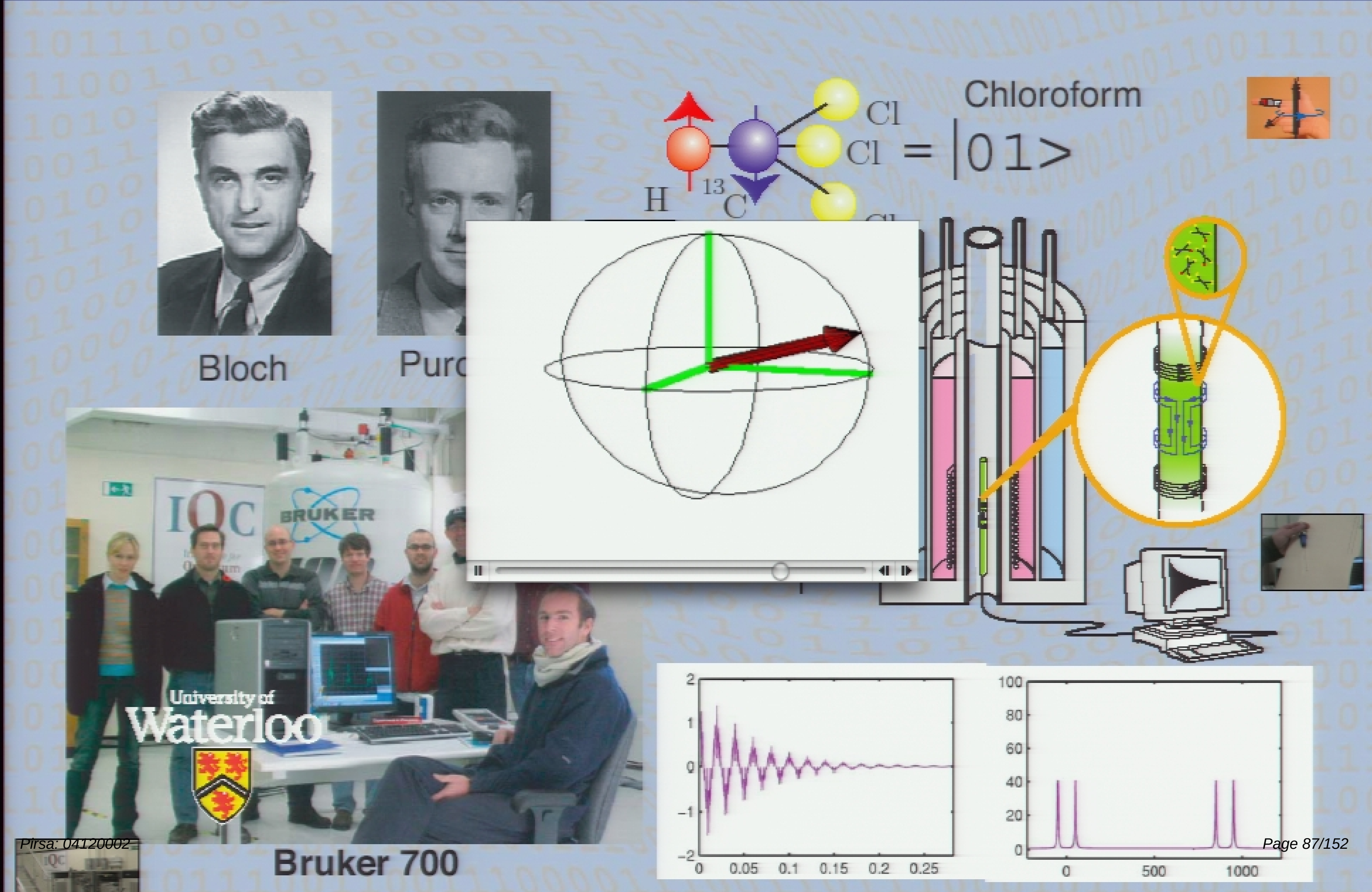


Bruker 700

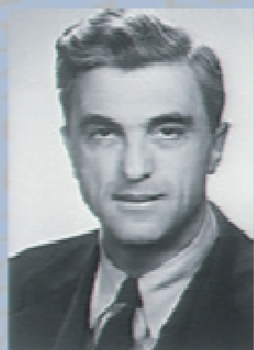




Nuclear Magnetic Resonance

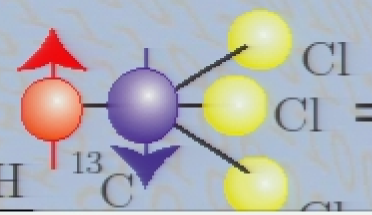


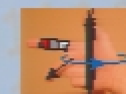
Nuclear Magnetic Resonance

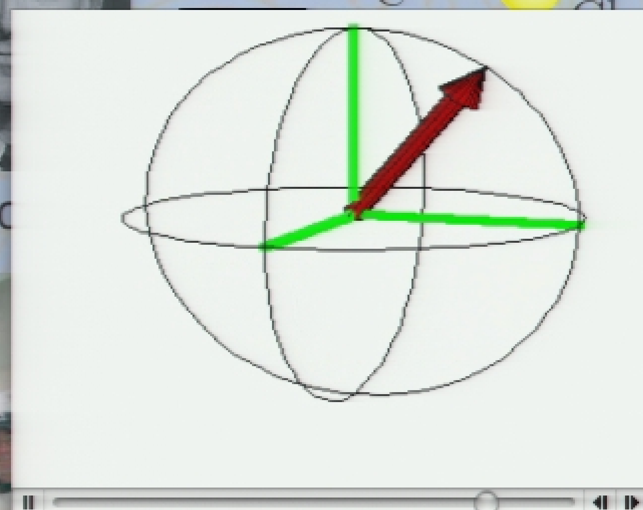


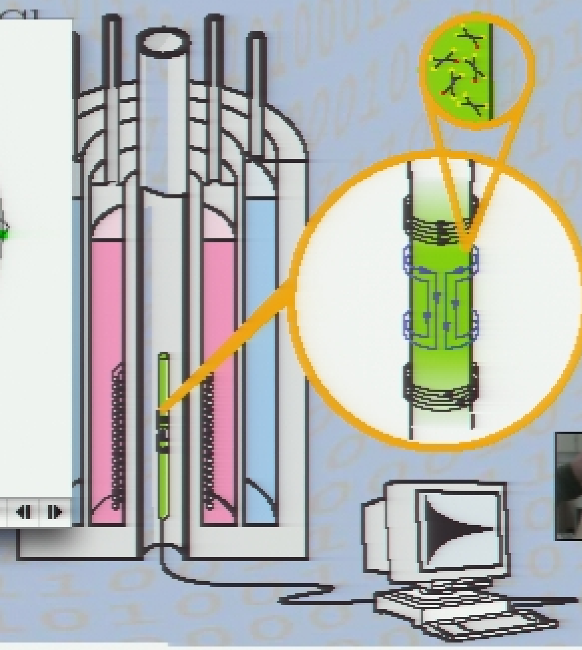
Bloch

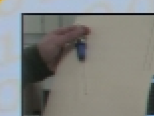
Purc

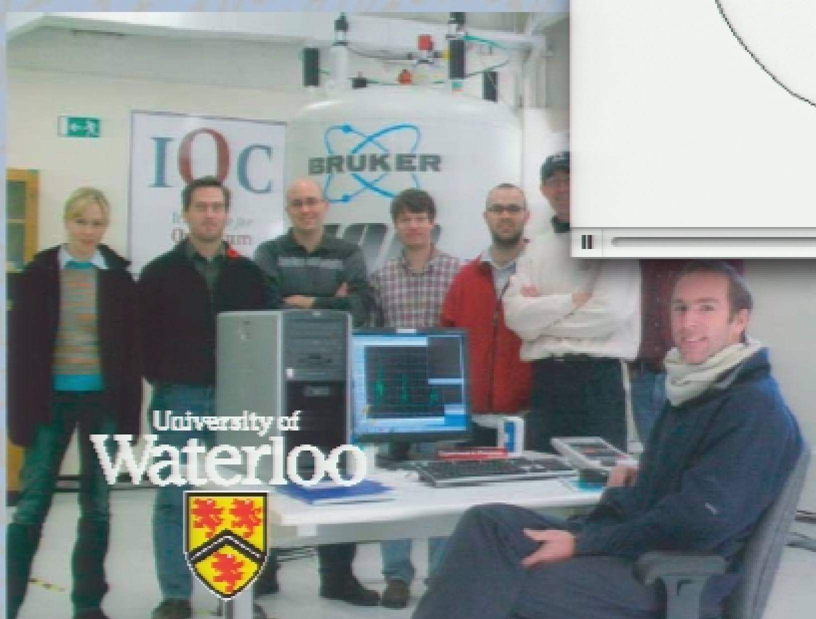


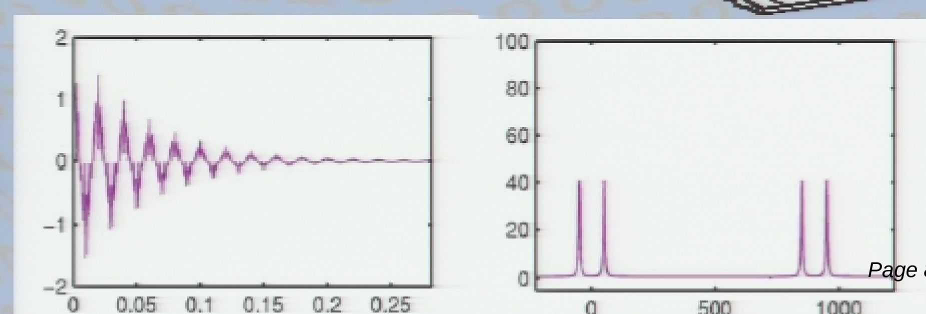


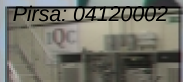






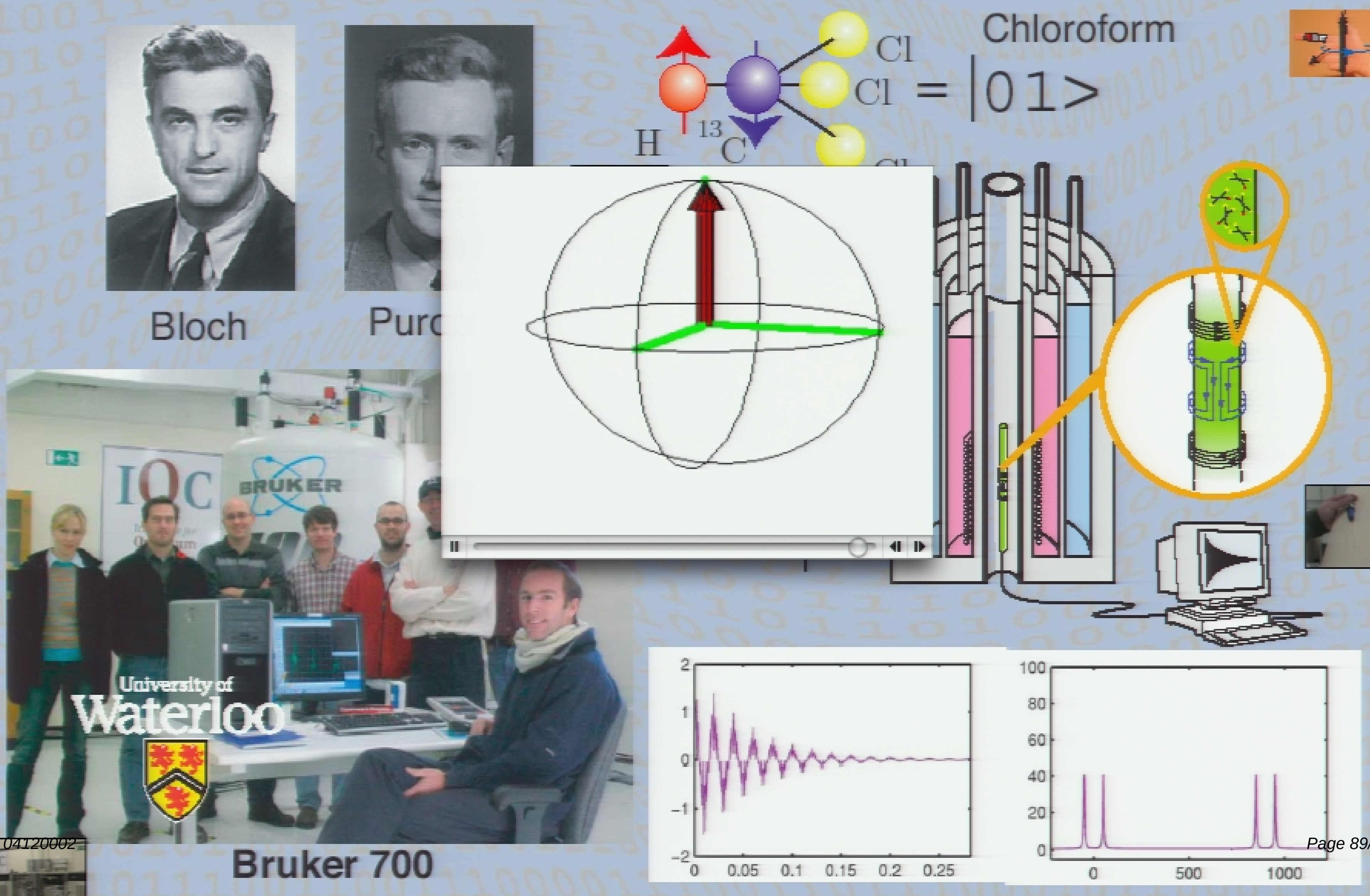






Bruker 700

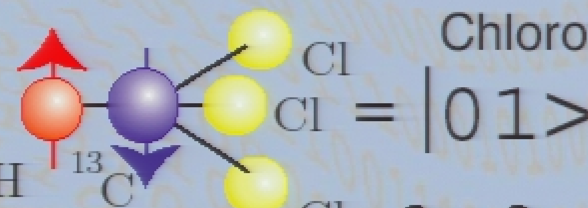
Nuclear Magnetic Resonance

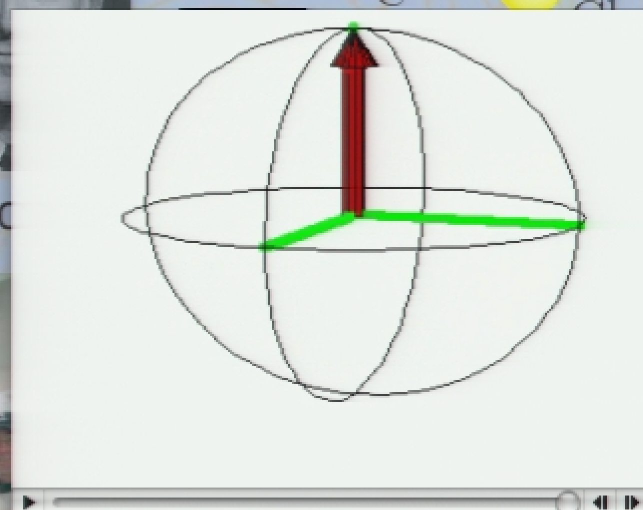


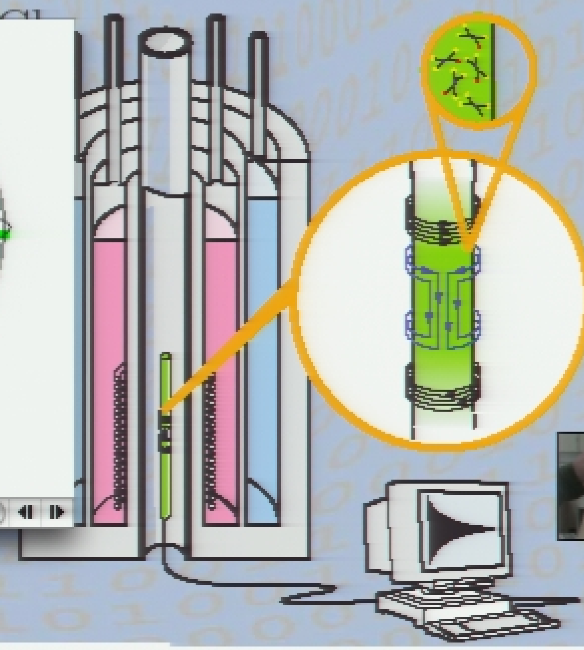
Nuclear Magnetic Resonance

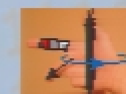
Bloch

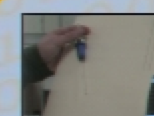
Purc

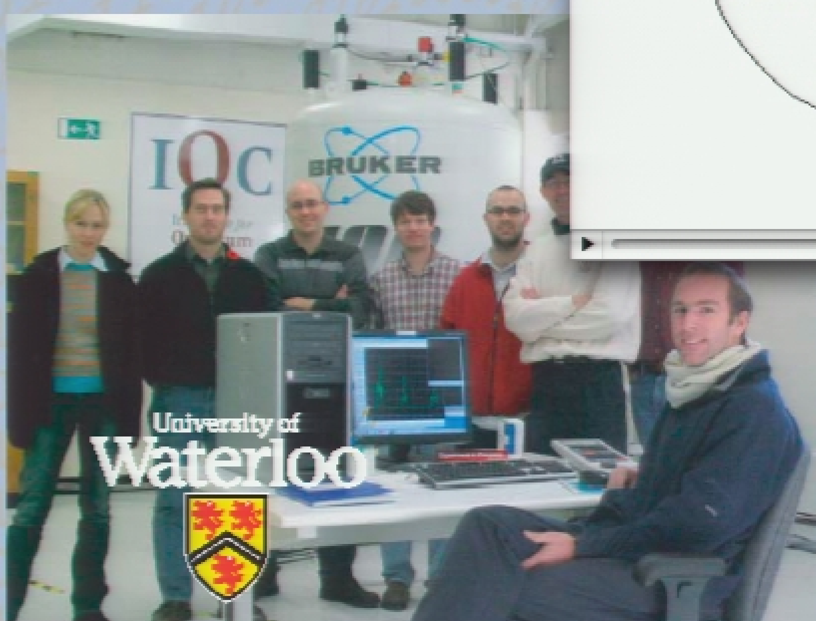




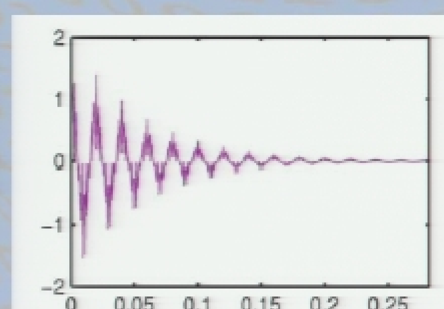


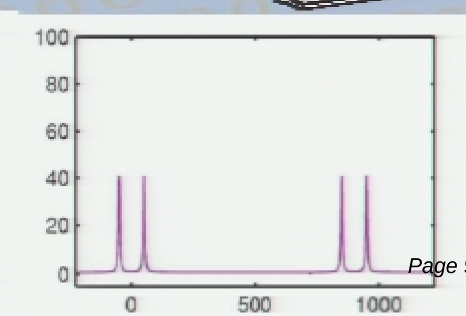




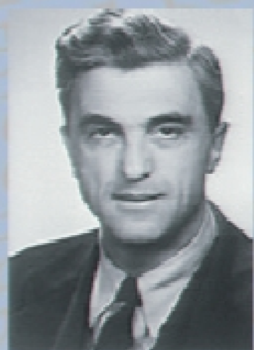


Bruker 700



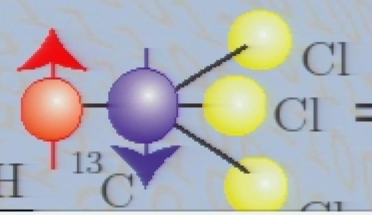


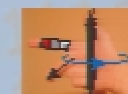
Nuclear Magnetic Resonance

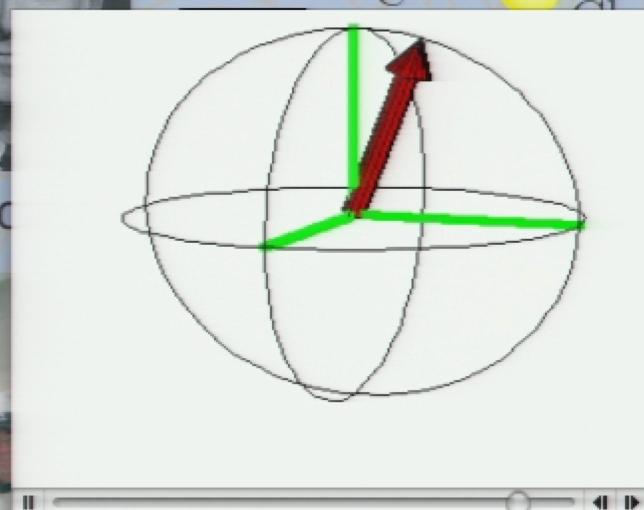


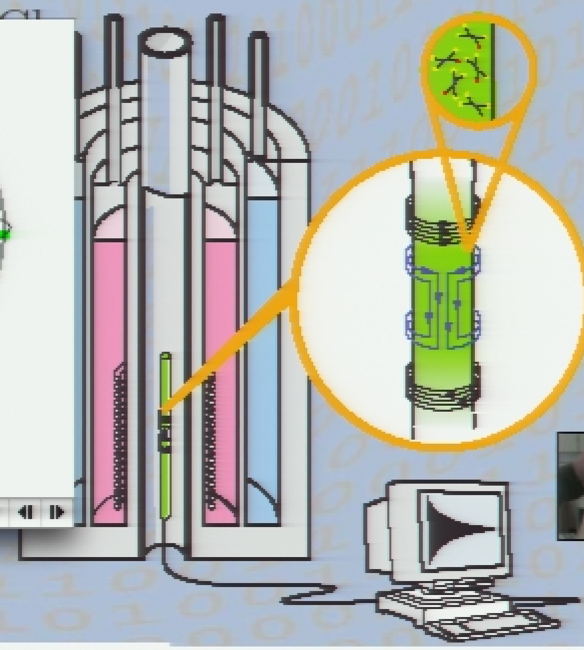
Bloch

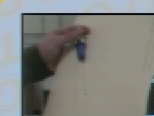
Purc

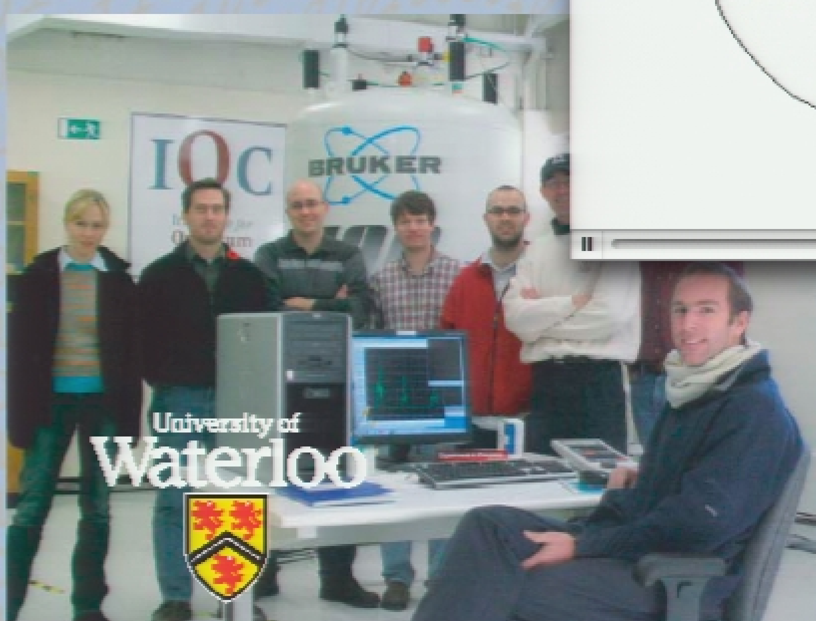


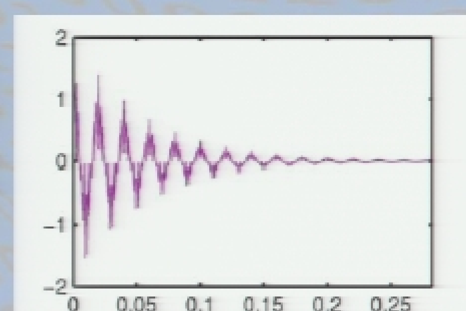


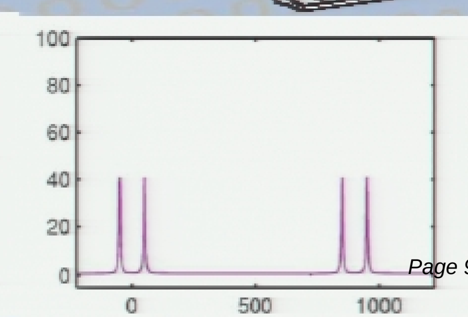


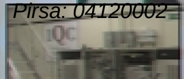






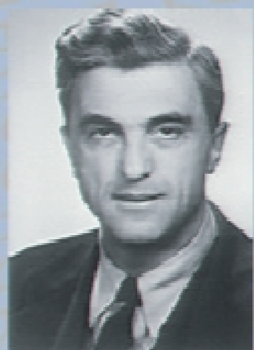






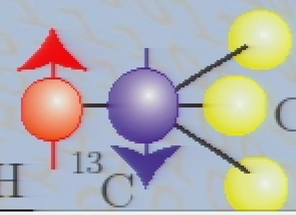
Bruker 700

Nuclear Magnetic Resonance



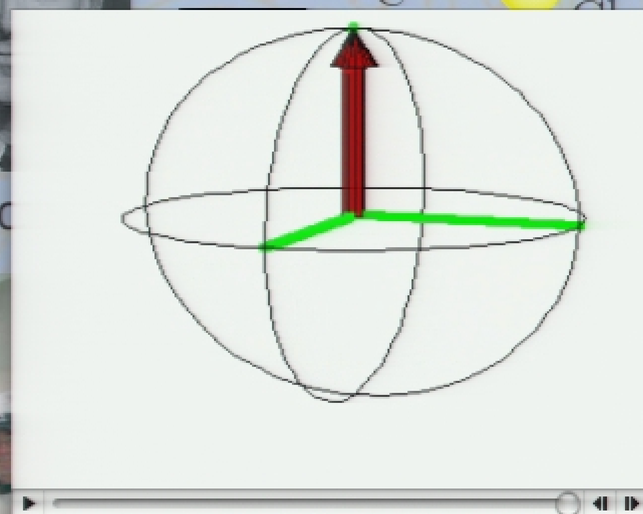
Bloch

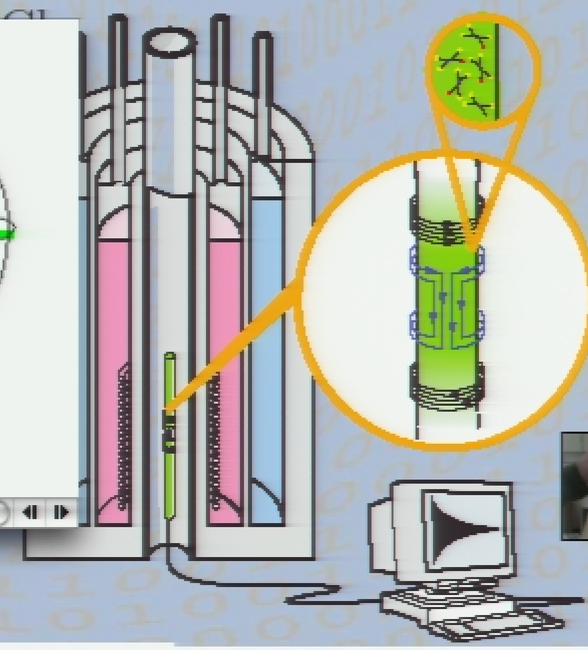
Purc

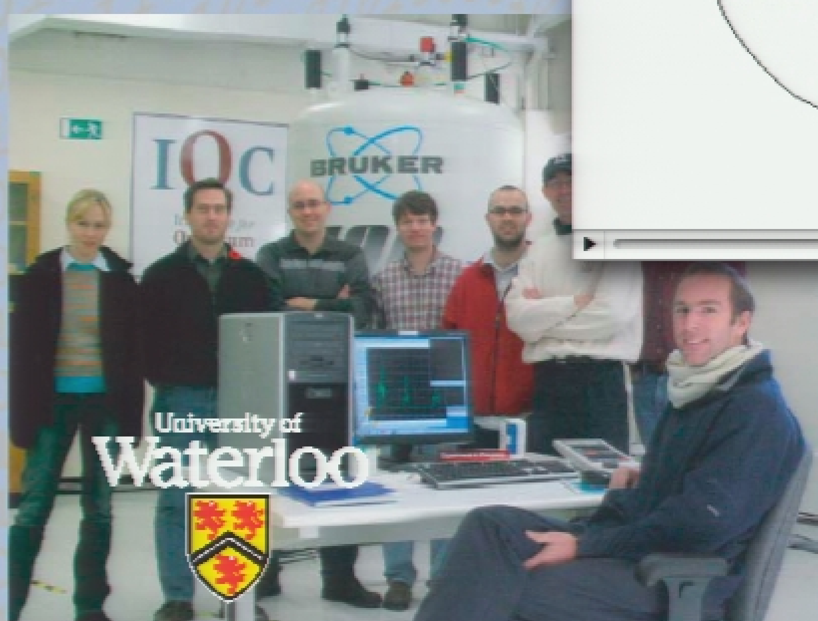


Chloroform

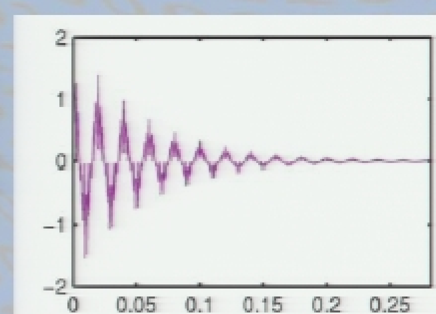
$= |01>$

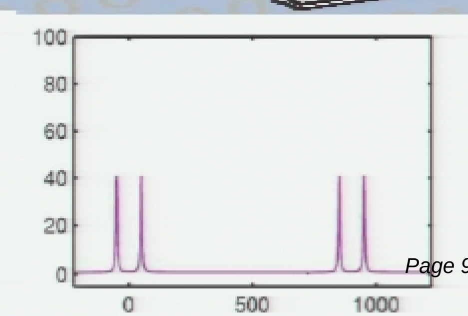




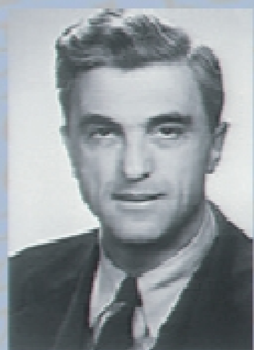


Bruker 700



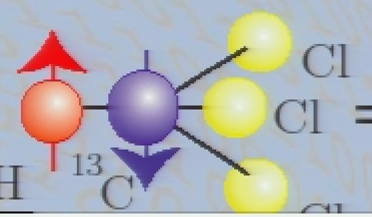


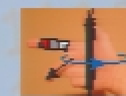
Nuclear Magnetic Resonance

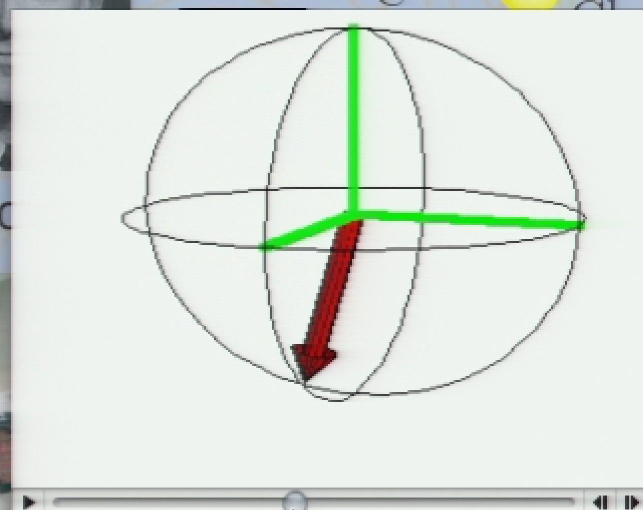


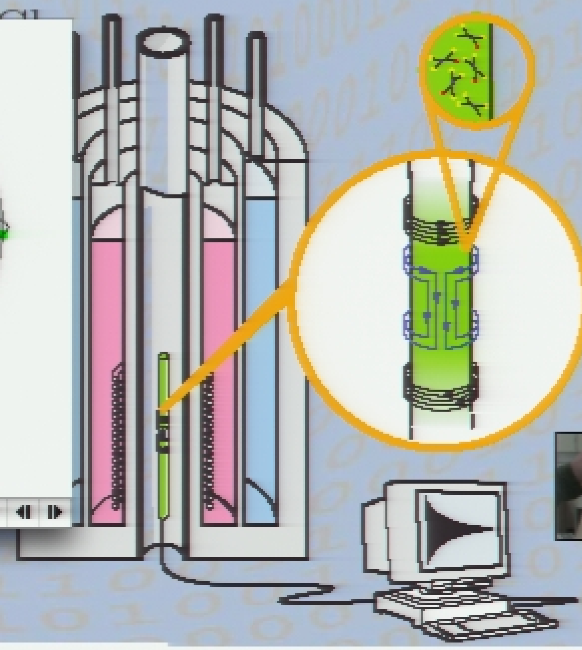
Bloch

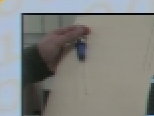
Purc

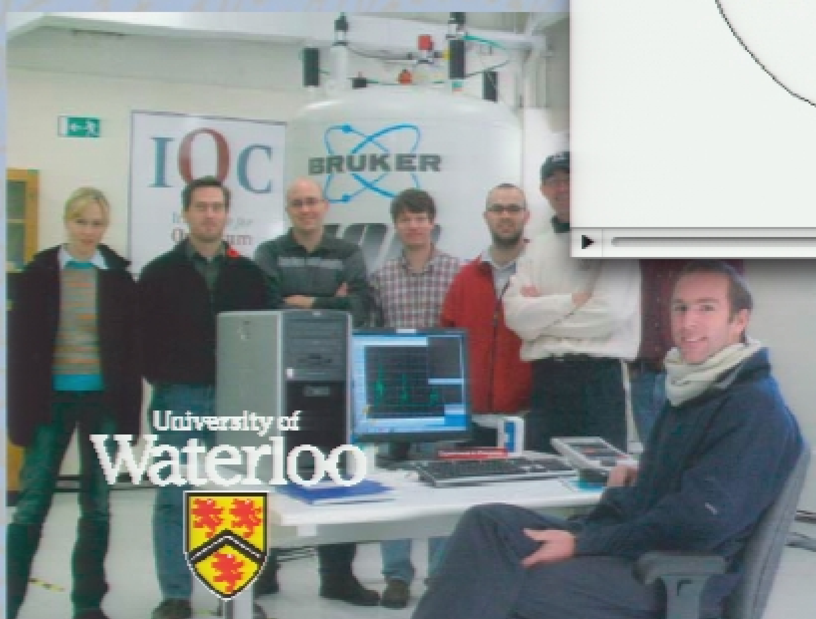




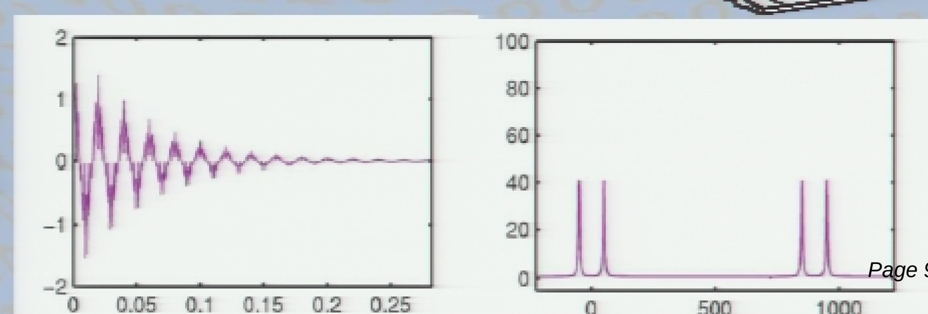




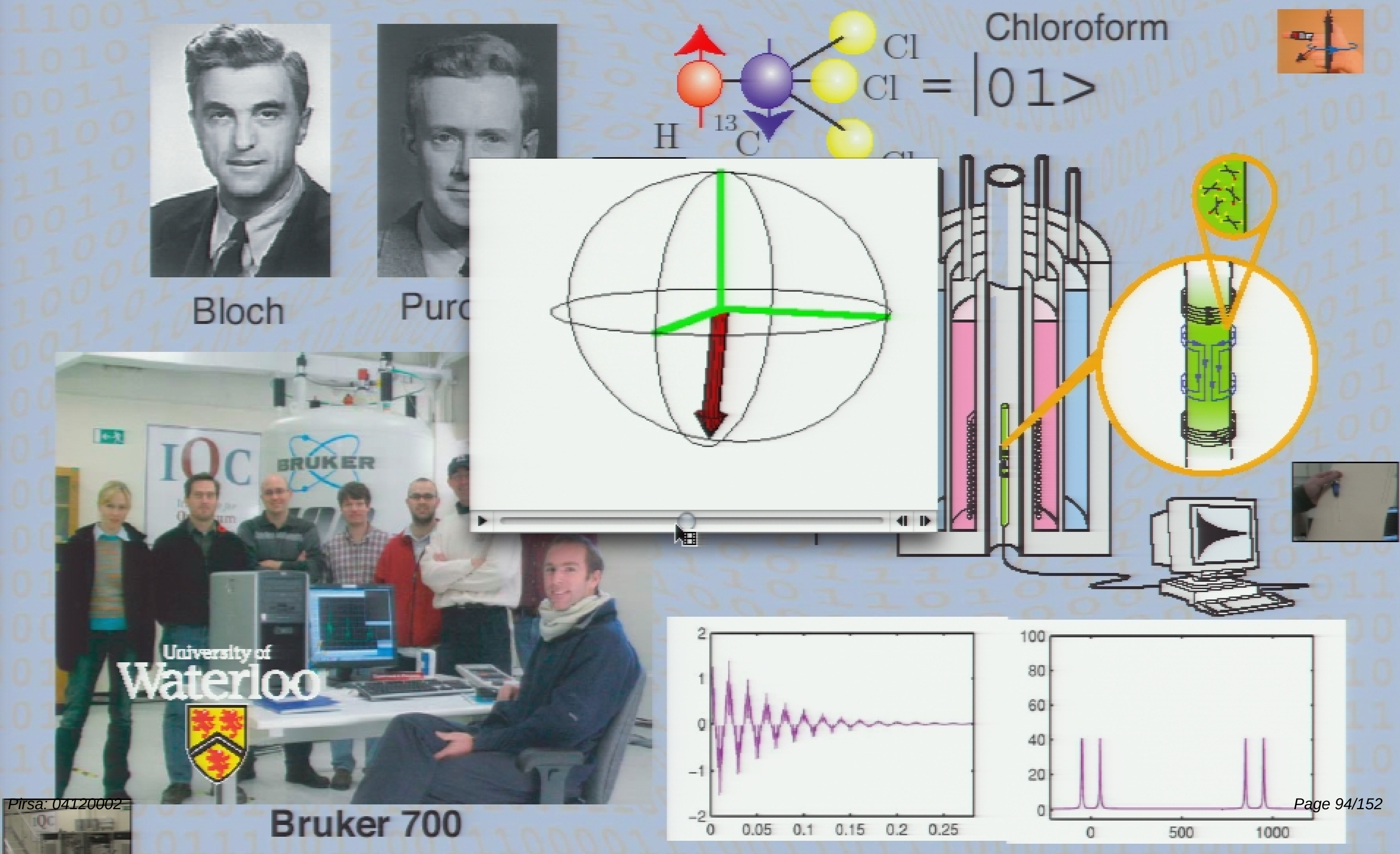




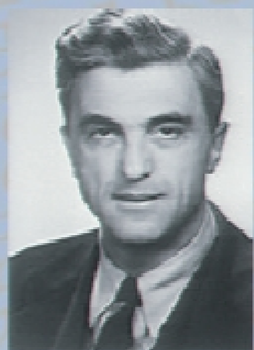
Bruker 700



Nuclear Magnetic Resonance

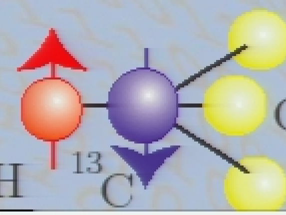


Nuclear Magnetic Resonance



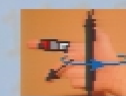
Bloch

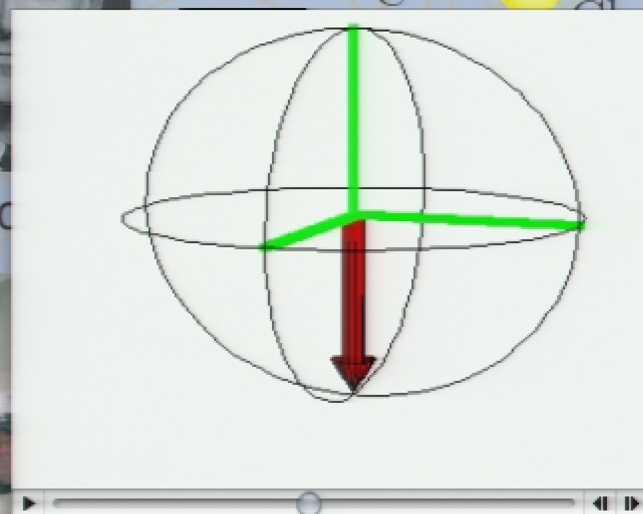
Purc

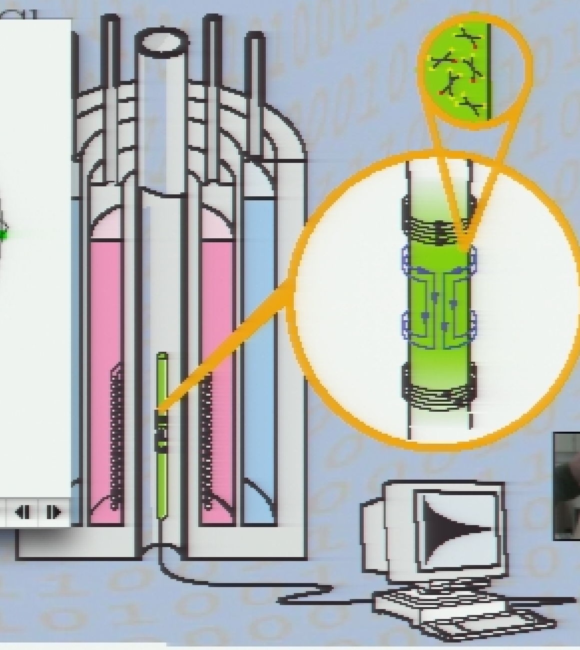


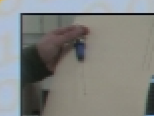
Chloroform

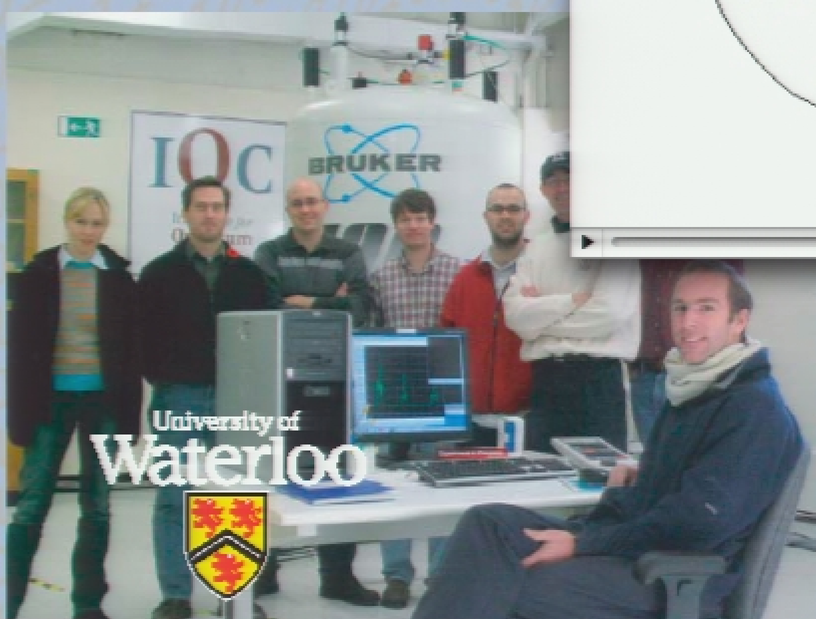
$= |01>$



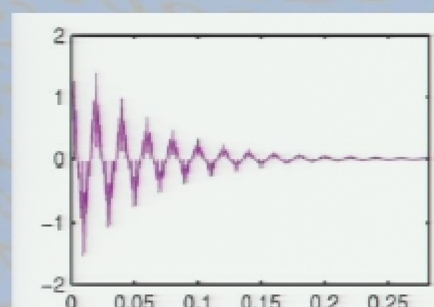


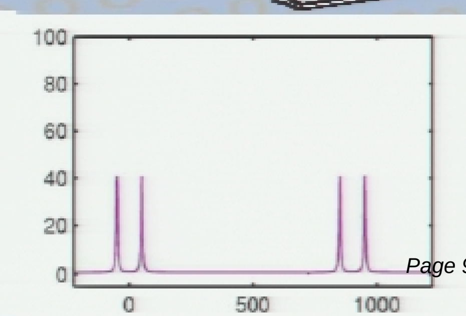


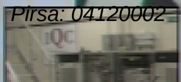




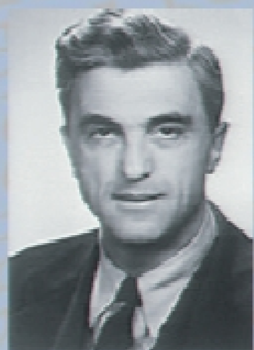
Bruker 700





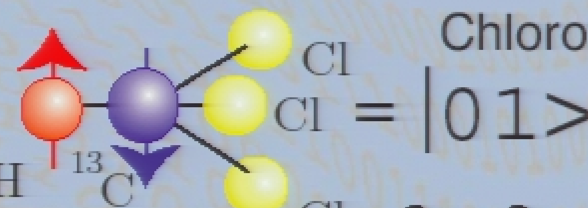


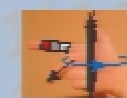
Nuclear Magnetic Resonance

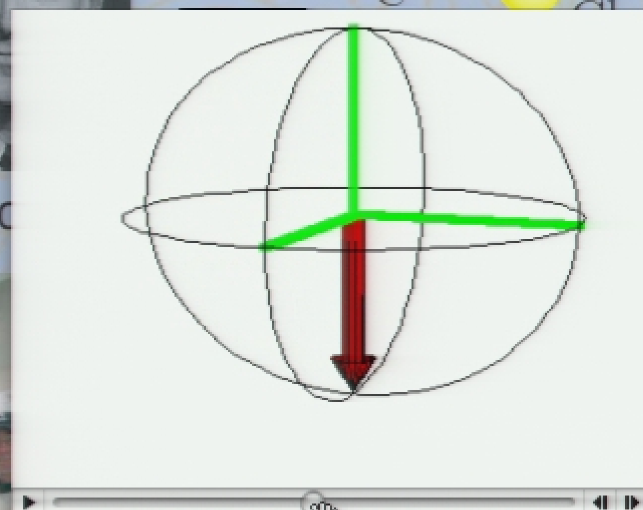


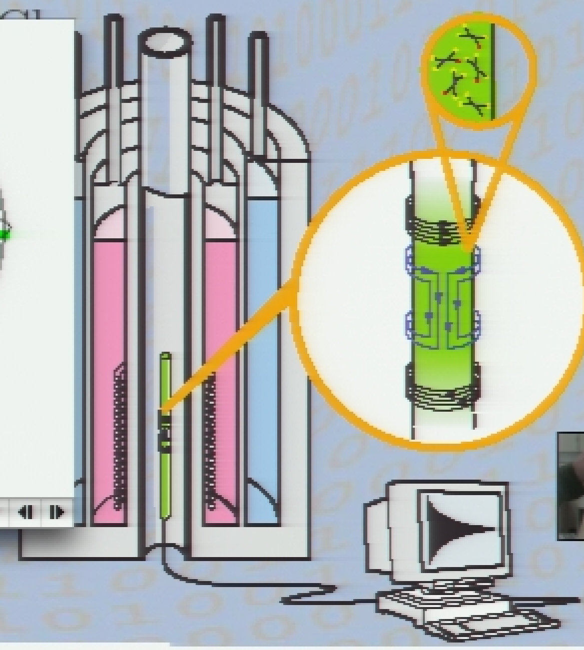
Bloch

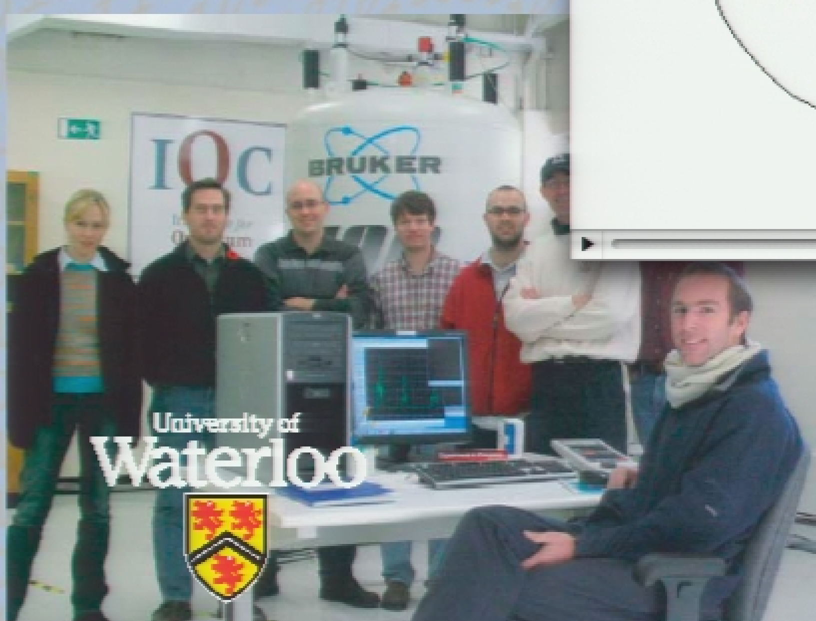
Purc



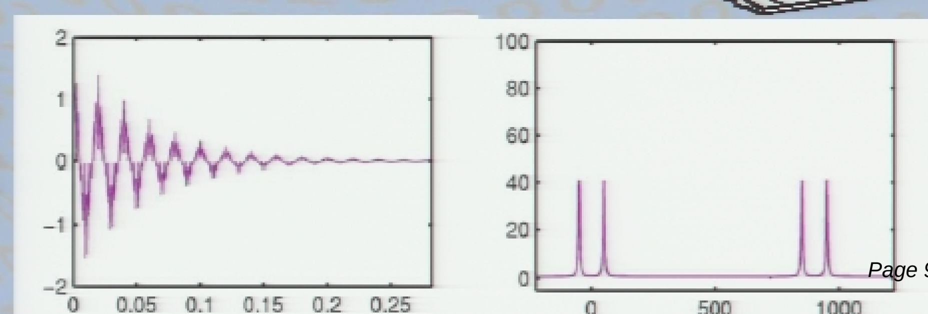




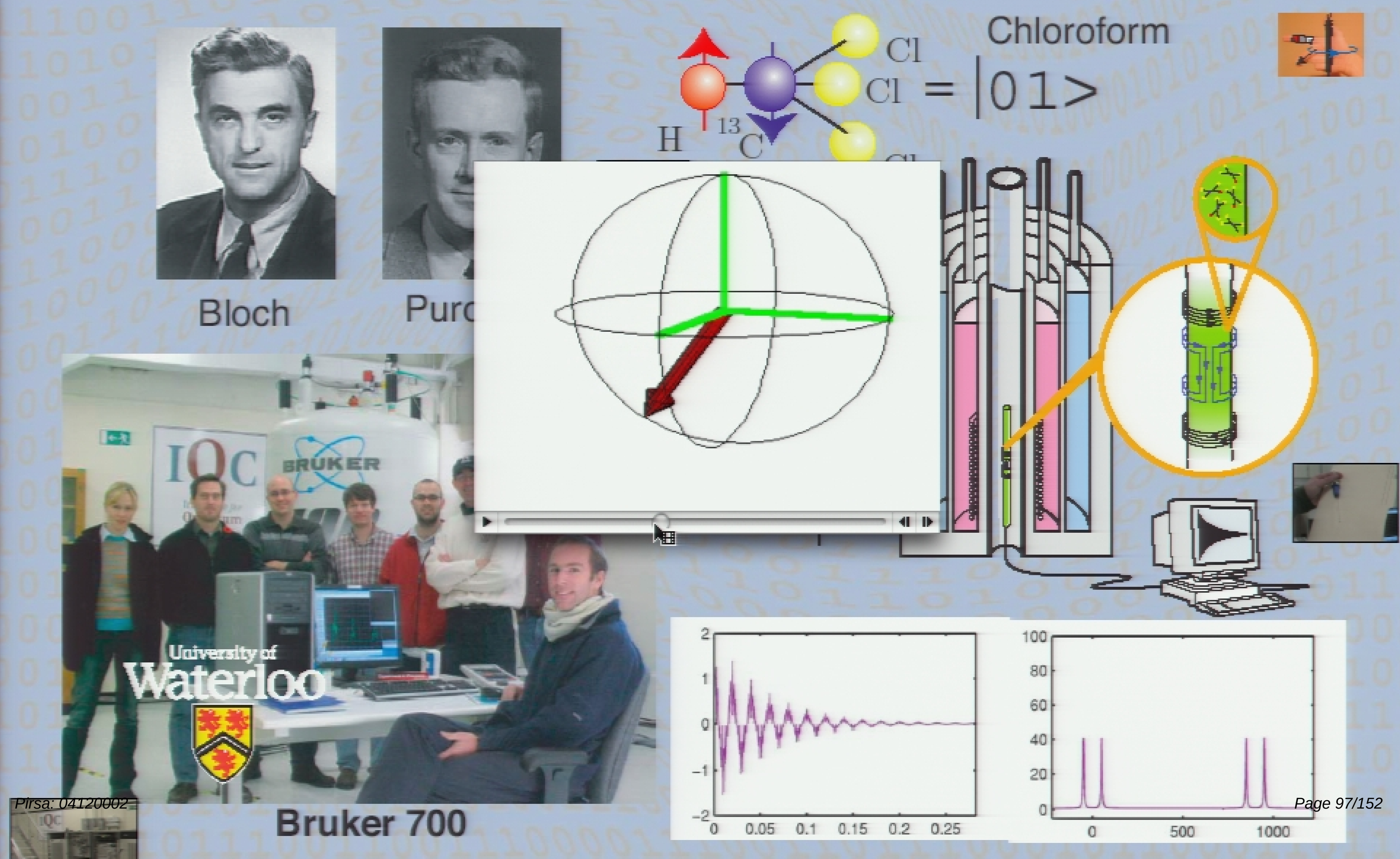




Bruker 700



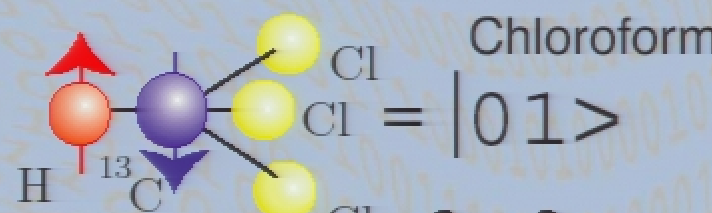
Nuclear Magnetic Resonance

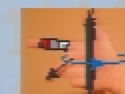


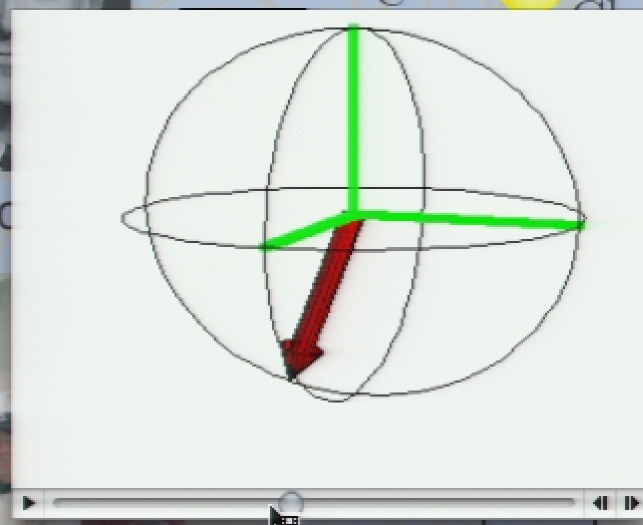
Nuclear Magnetic Resonance

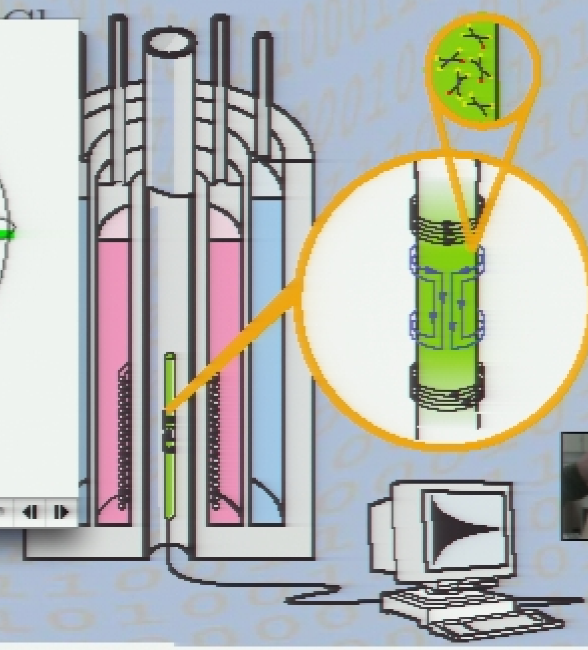
Bloch

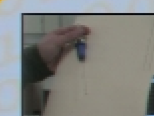
Purc

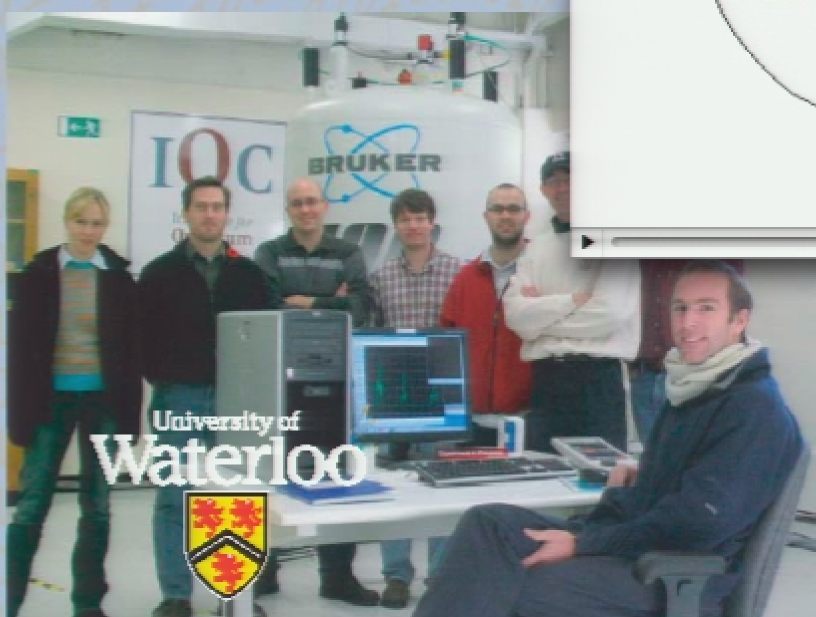




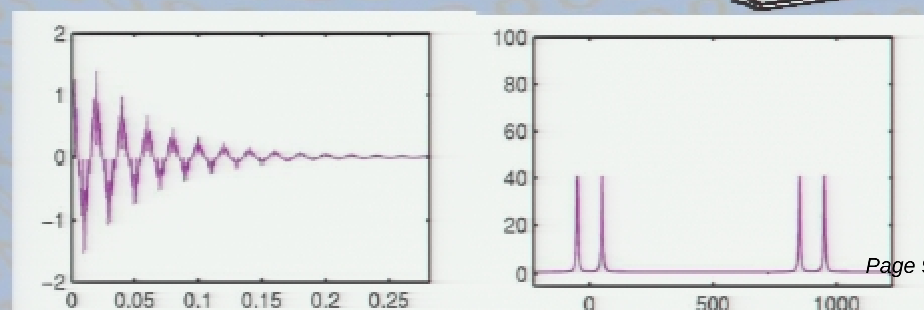




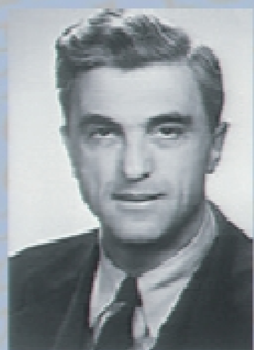




Bruker 700

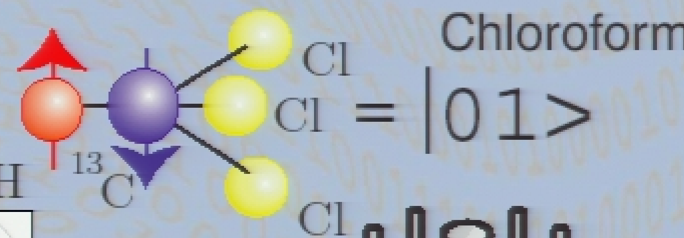


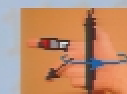
Nuclear Magnetic Resonance

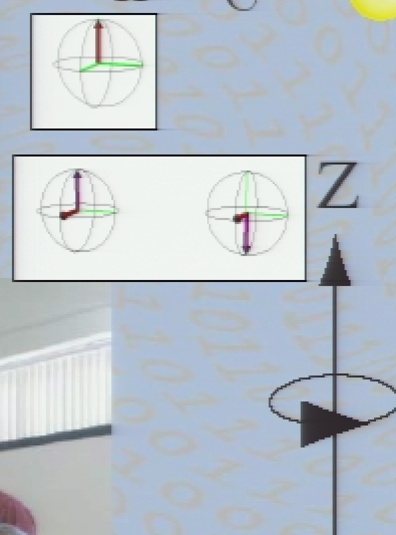


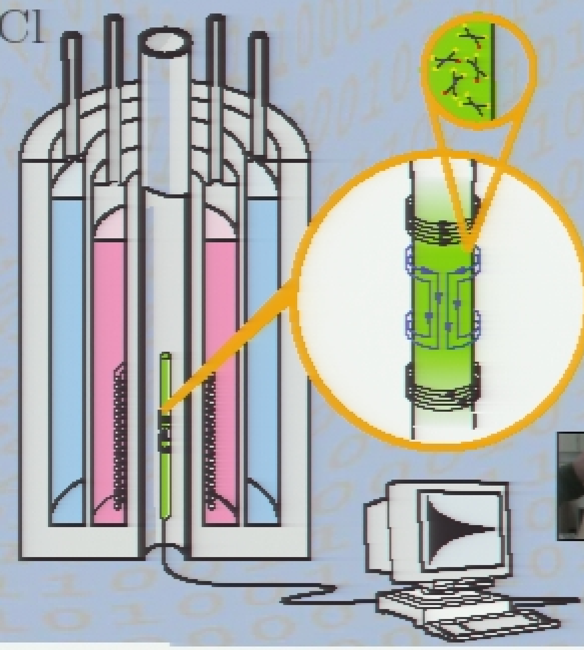
Bloch

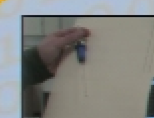
Purcell



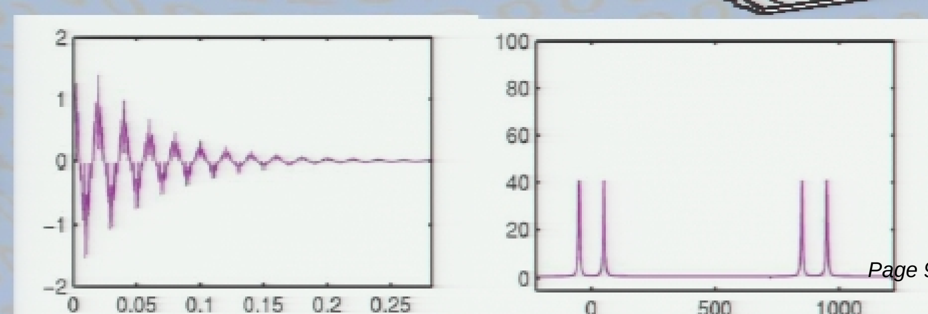




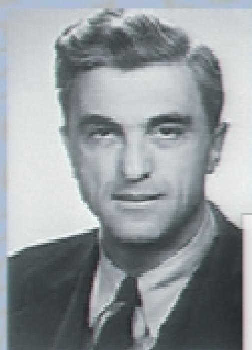




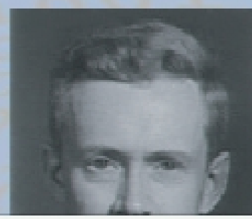
Bruker 700

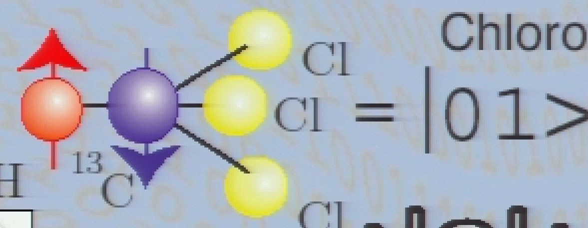


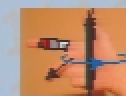
Nuclear Magnetic Resonance

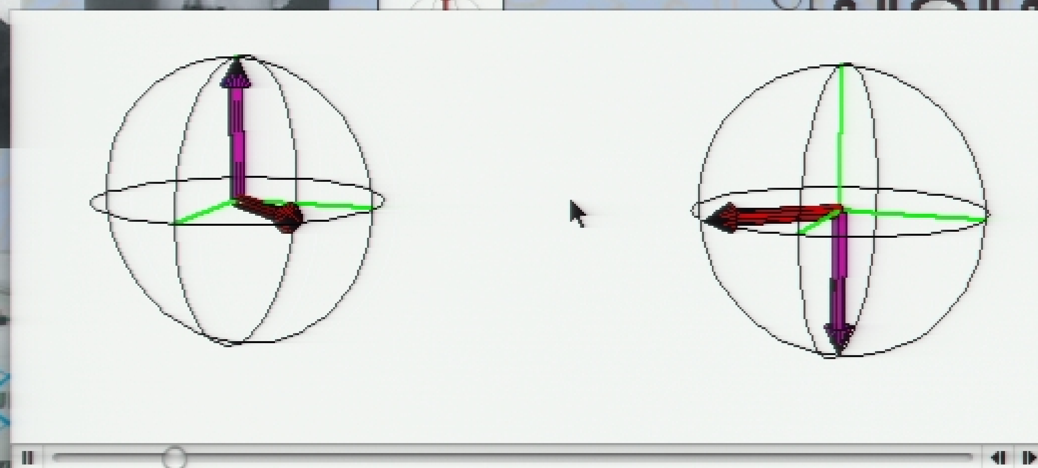


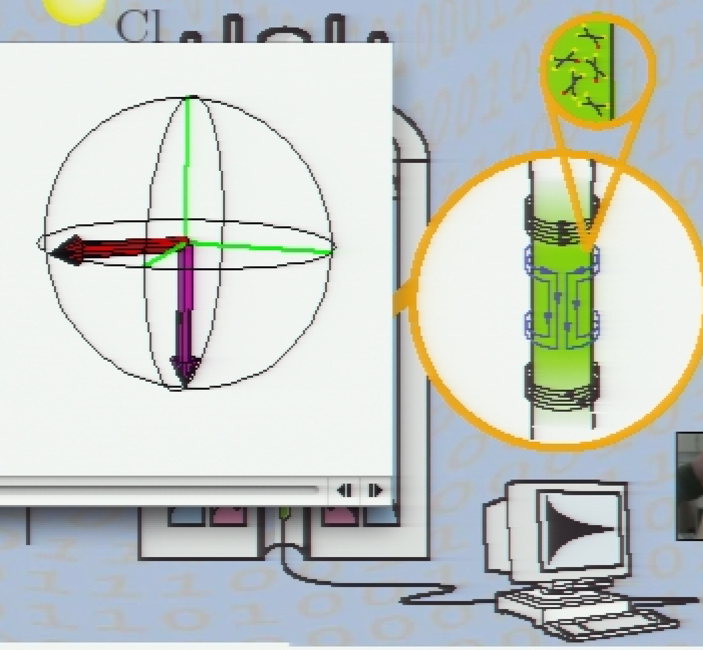
Bloch

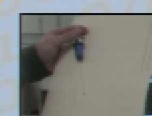


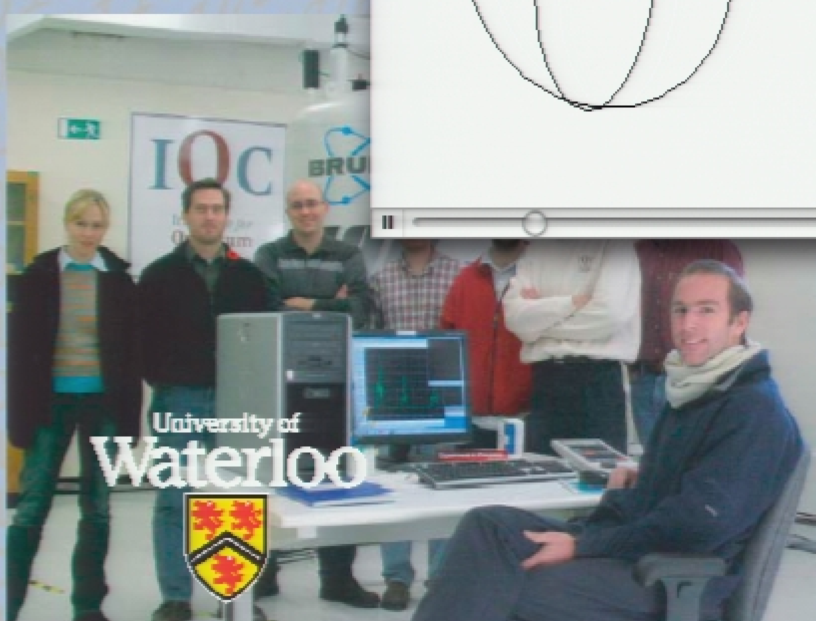




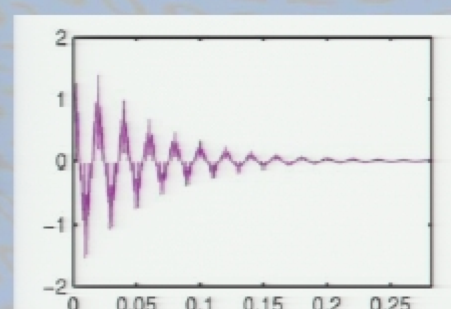


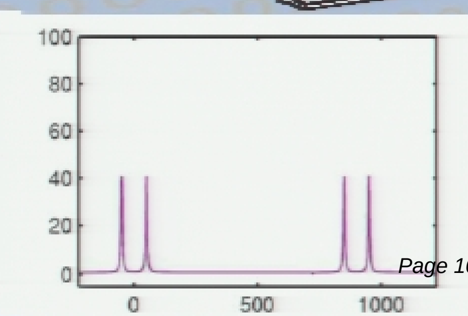




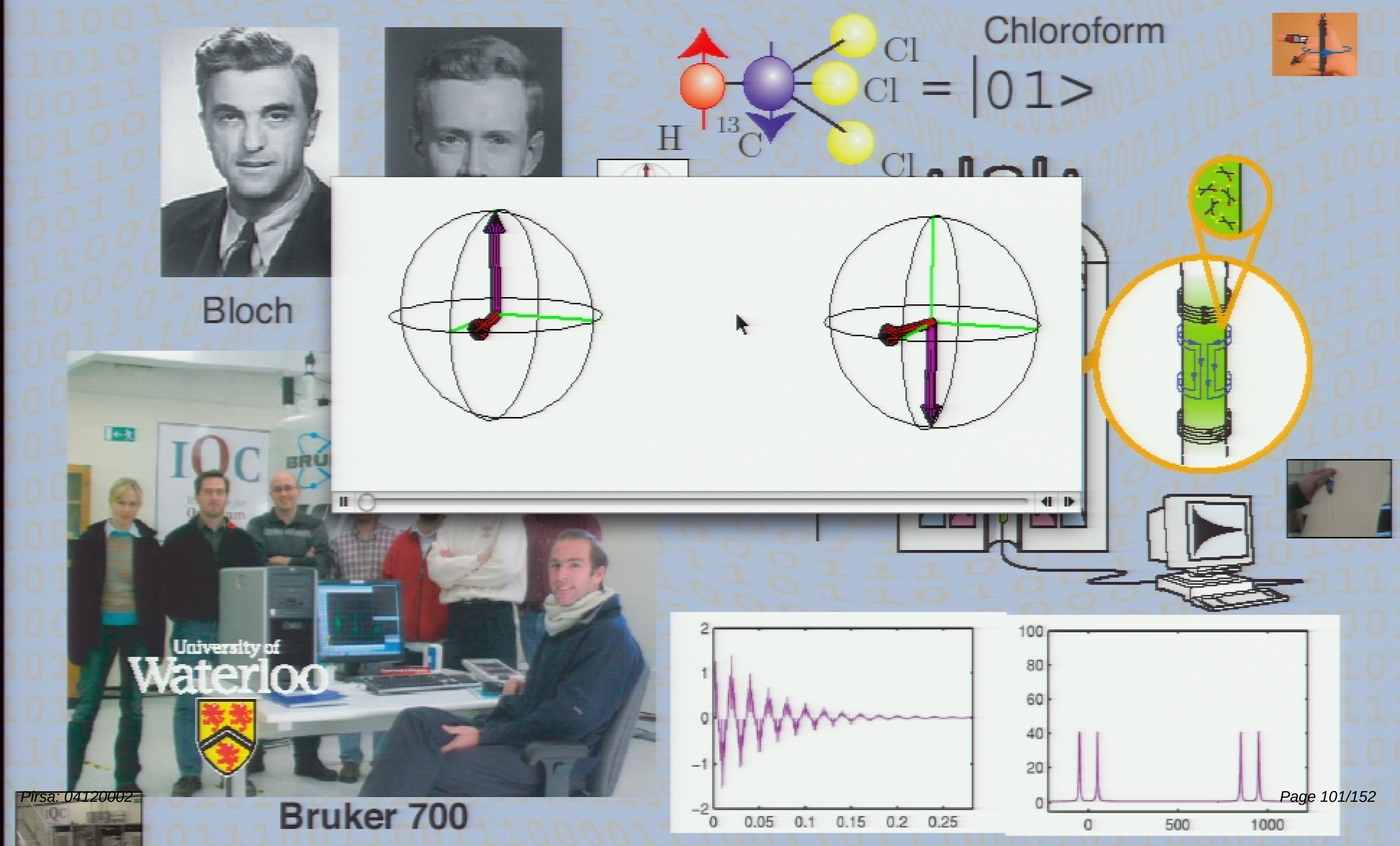


Bruker 700

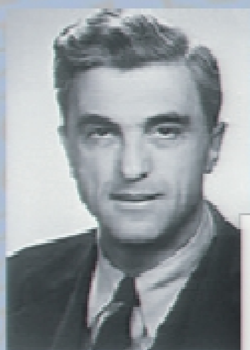




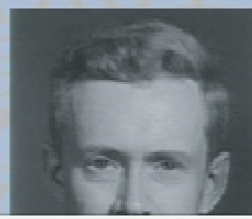
Nuclear Magnetic Resonance



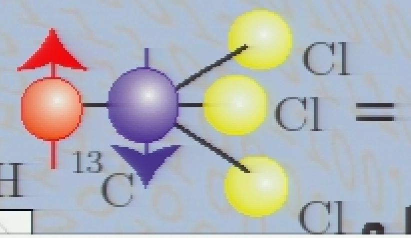
Nuclear Magnetic Resonance

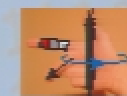


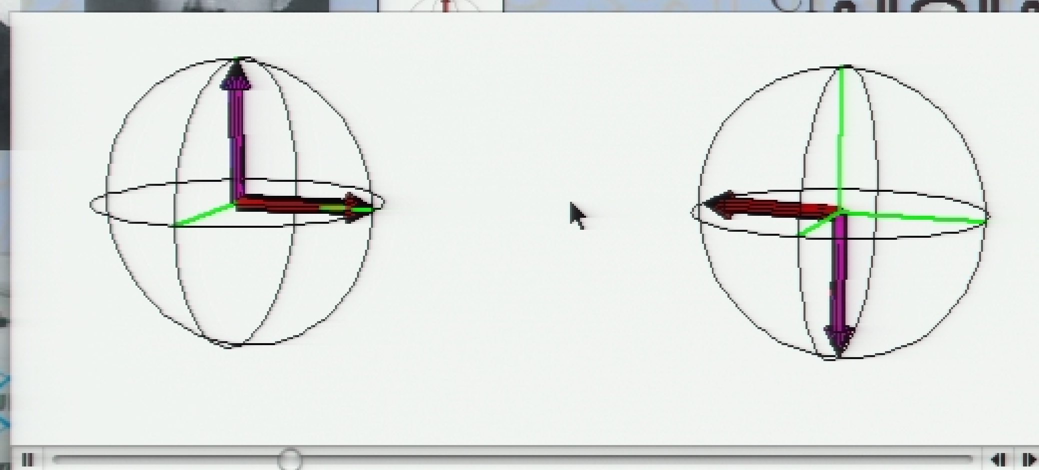
Bloch

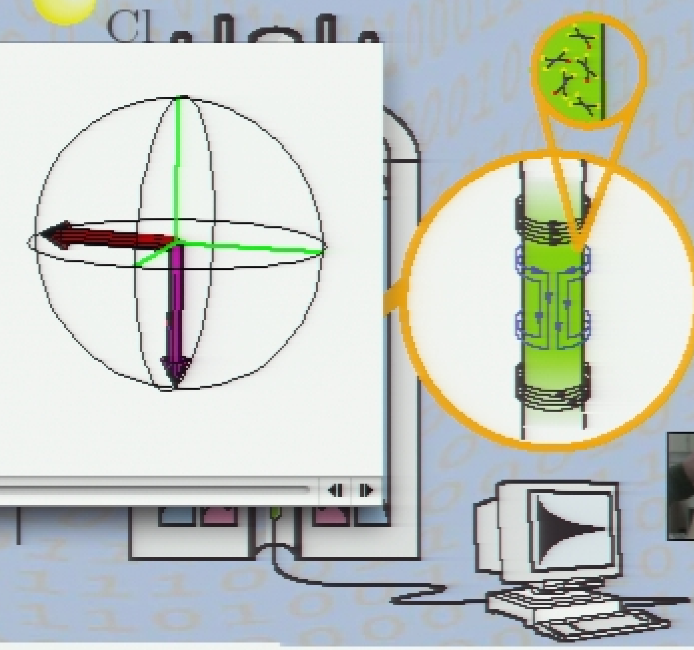


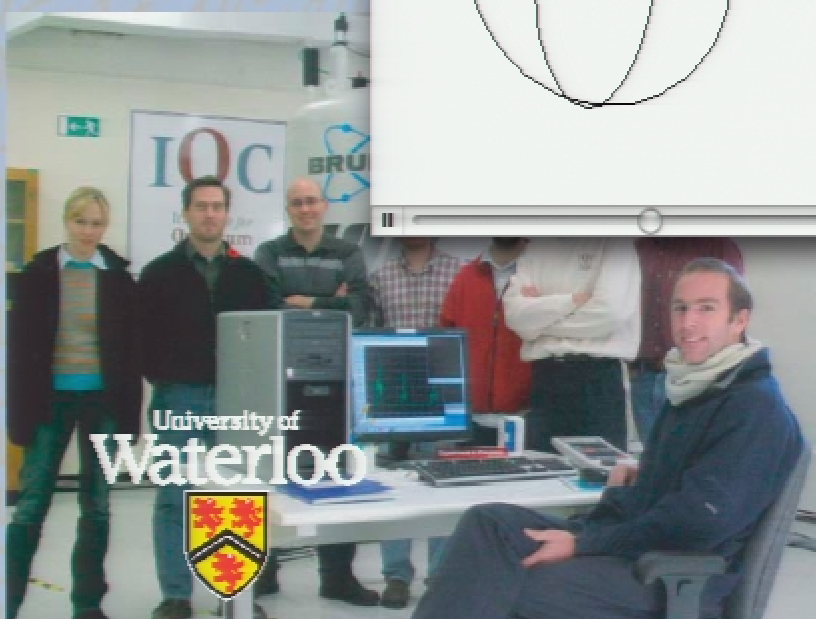
Chloroform



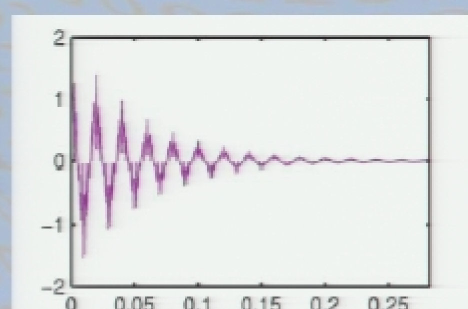


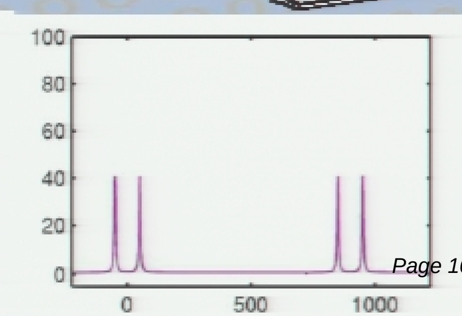


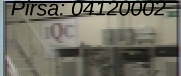




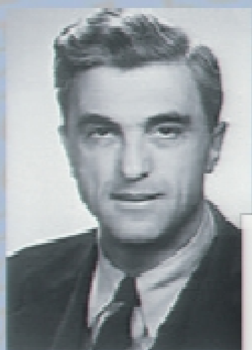
Bruker 700



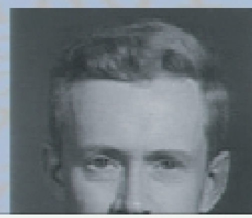


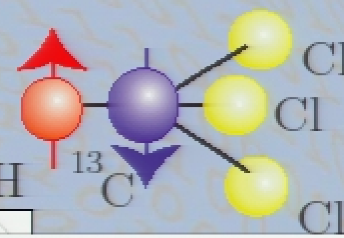


Nuclear Magnetic Resonance

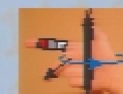


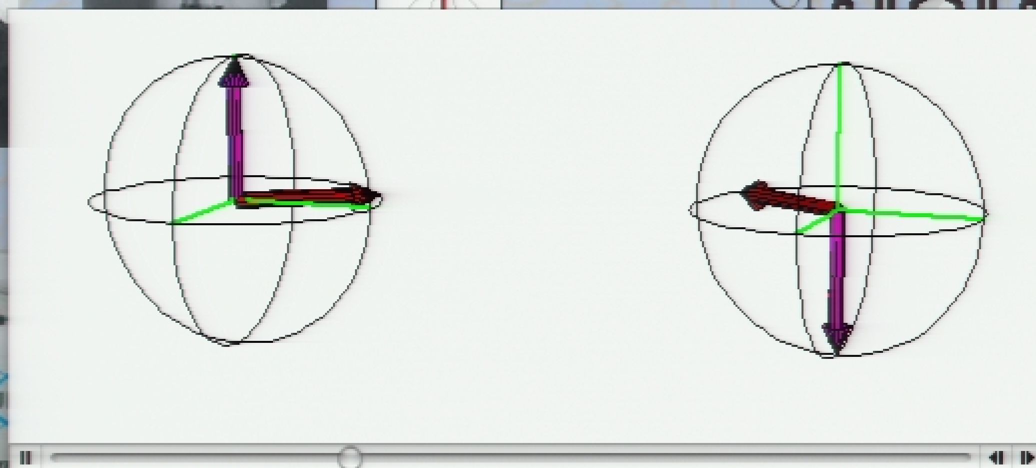
Bloch

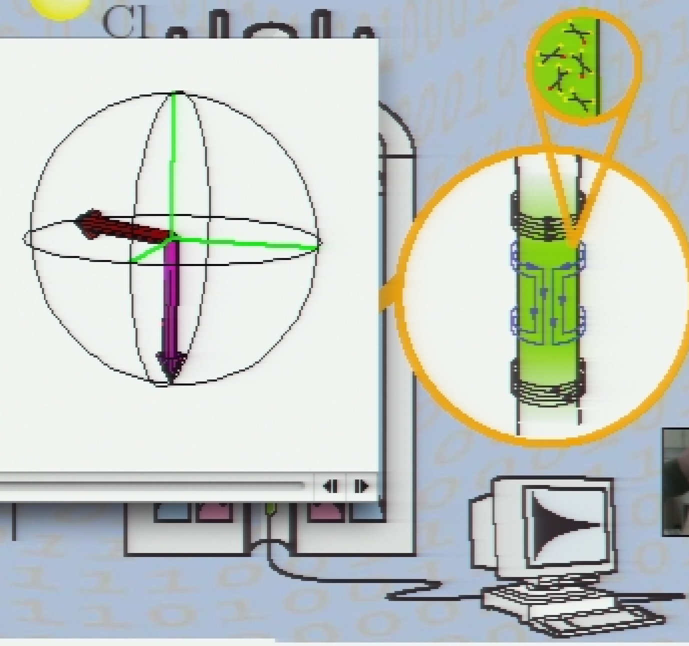


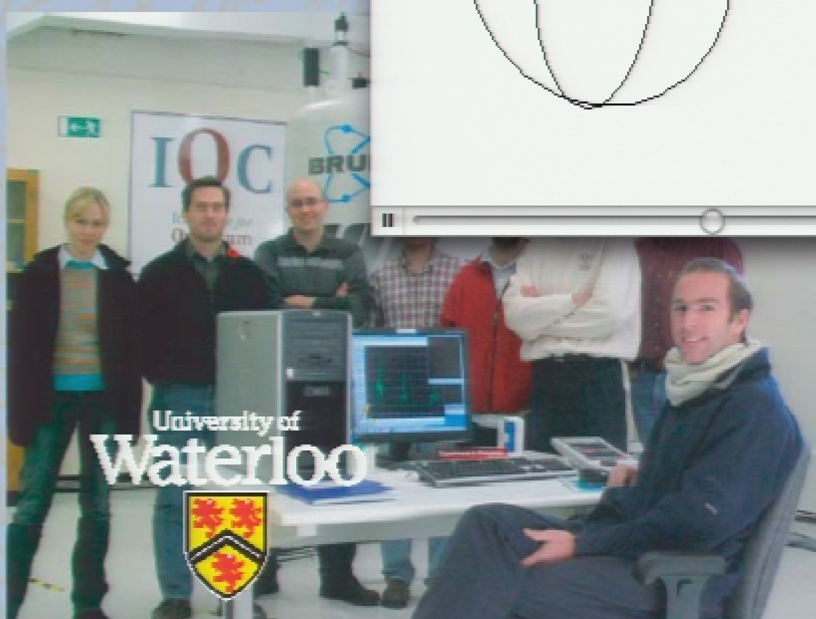


Chloroform $= |01>$

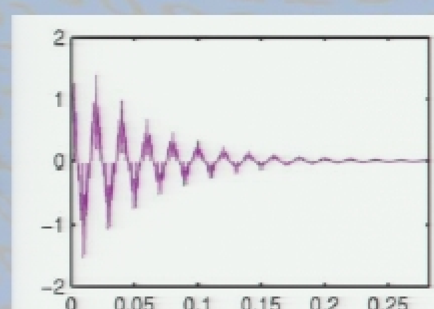


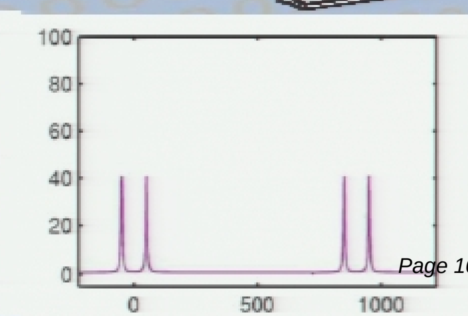


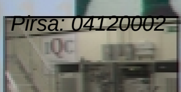




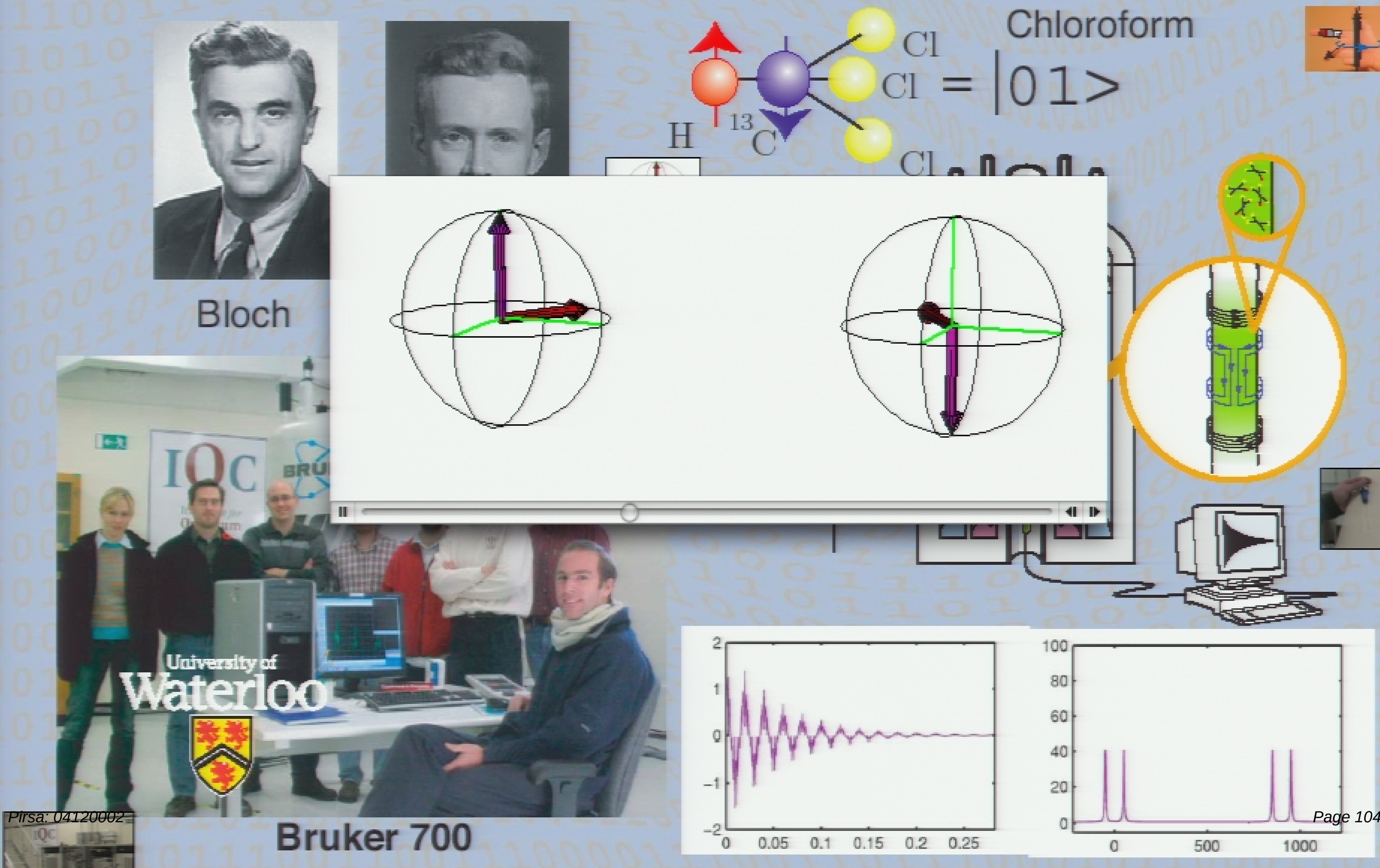
Bruker 700



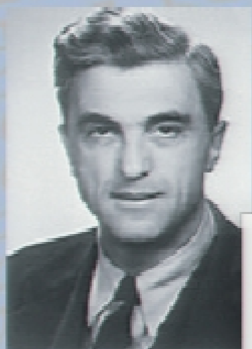




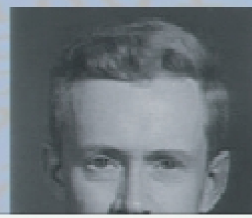
Nuclear Magnetic Resonance

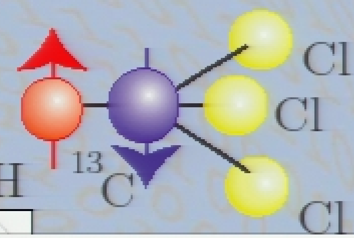


Nuclear Magnetic Resonance

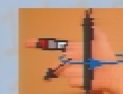


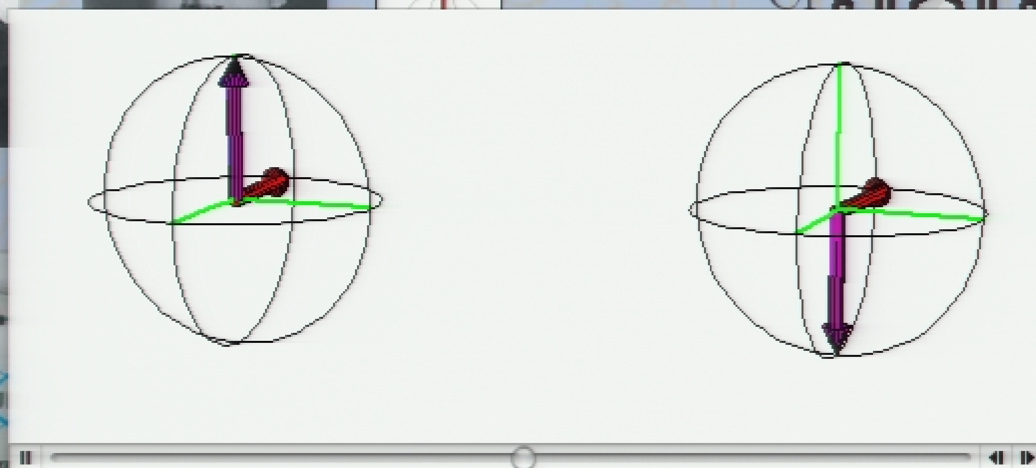
Bloch

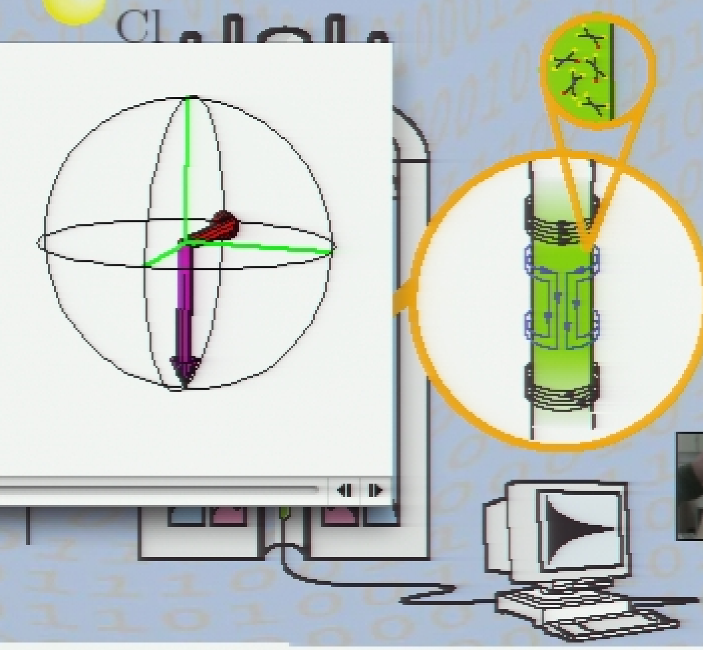


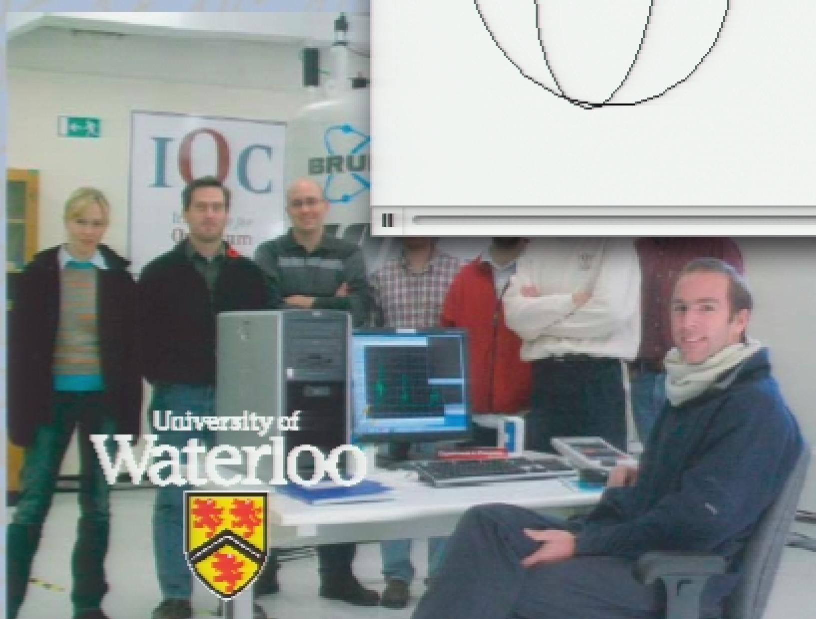


Chloroform $= |01>$

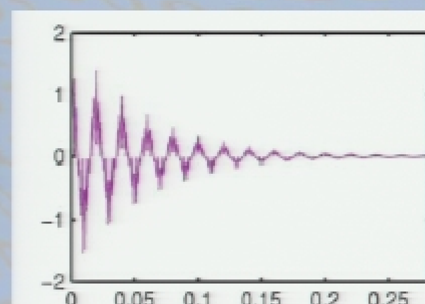


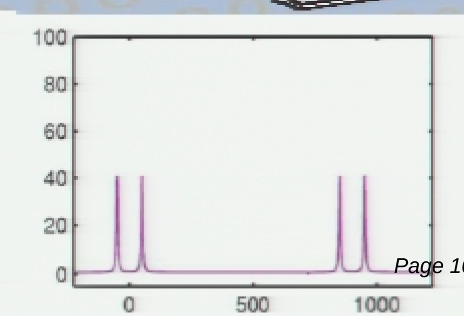


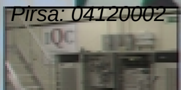




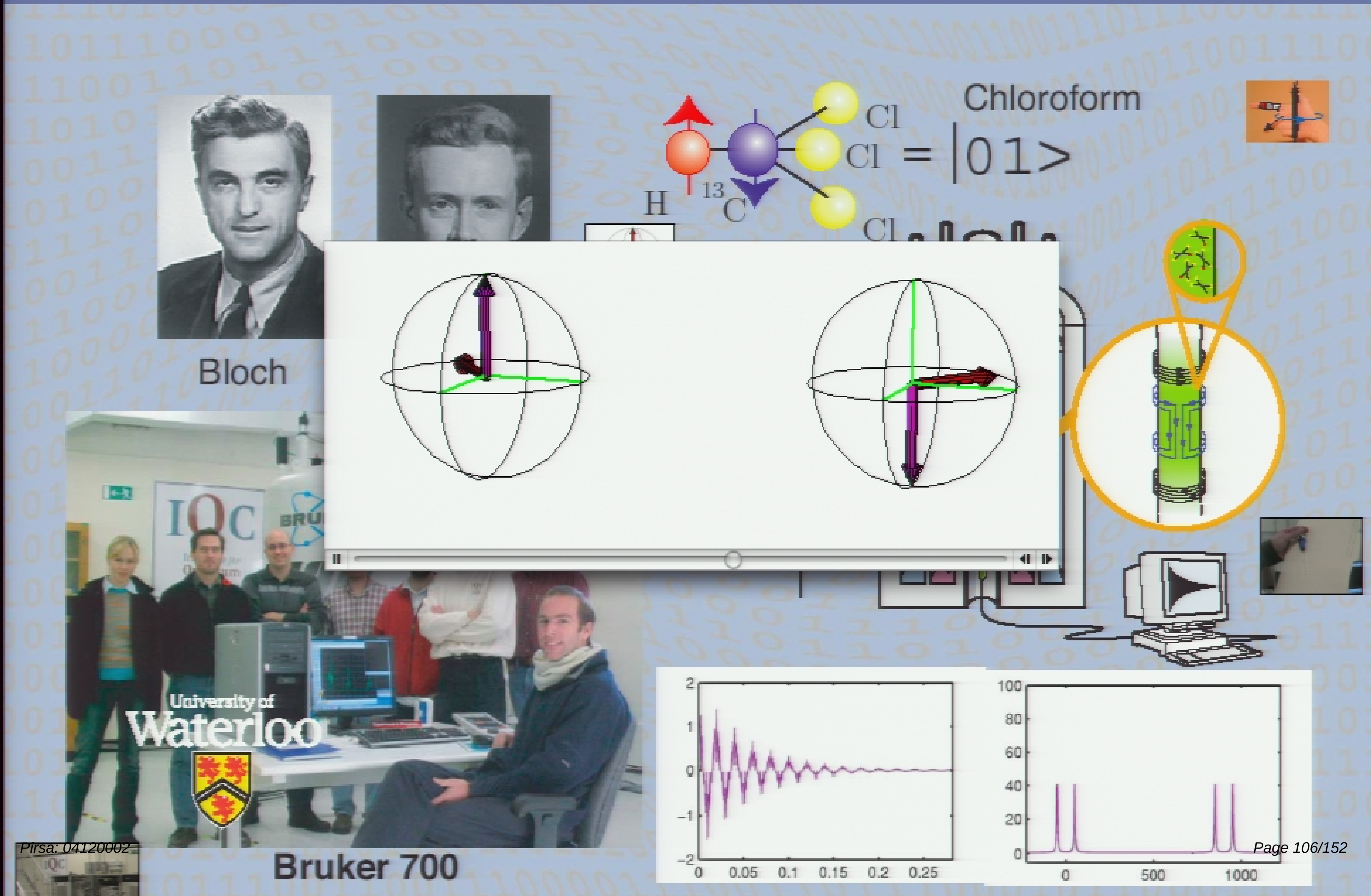
Bruker 700



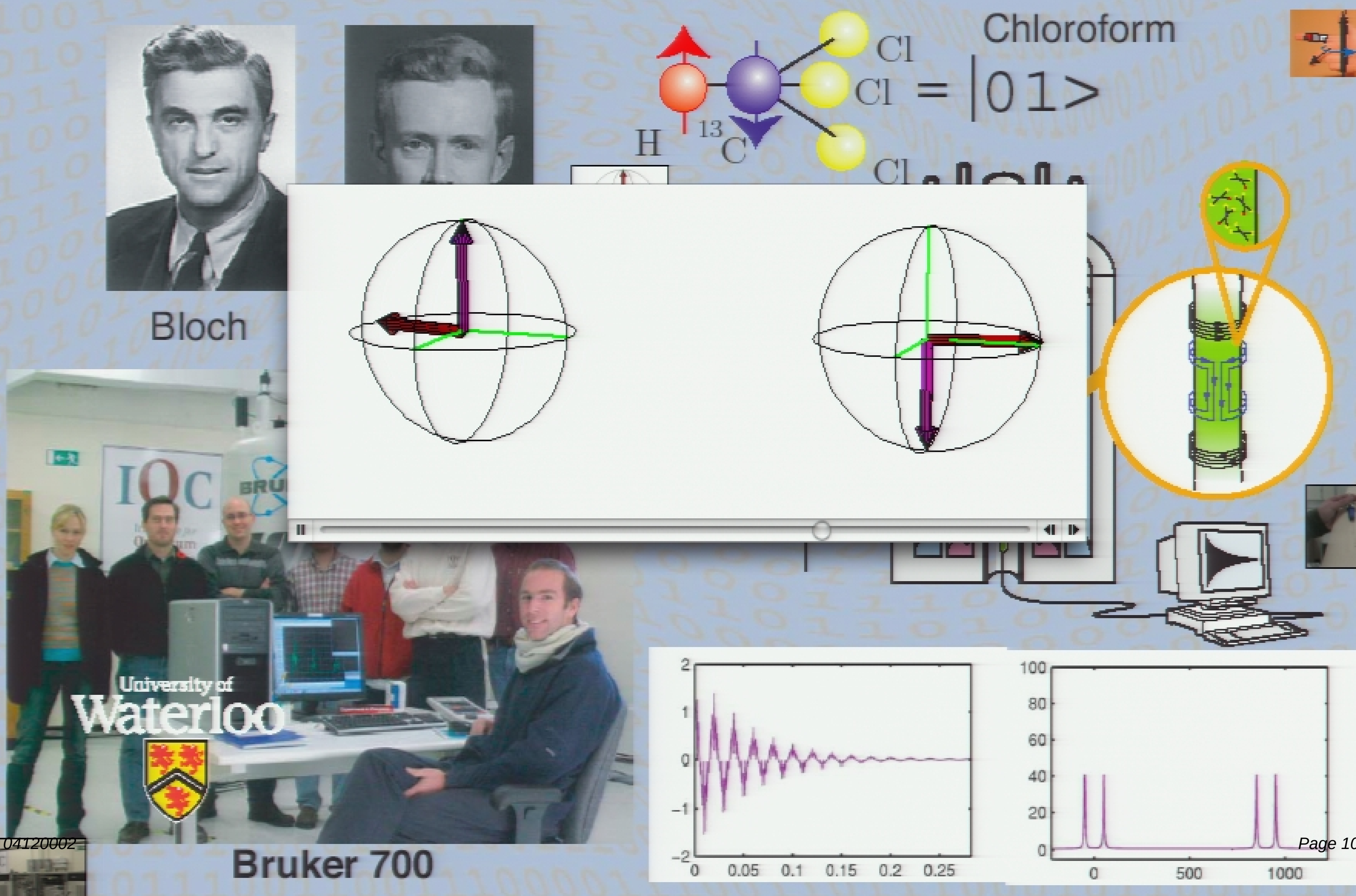




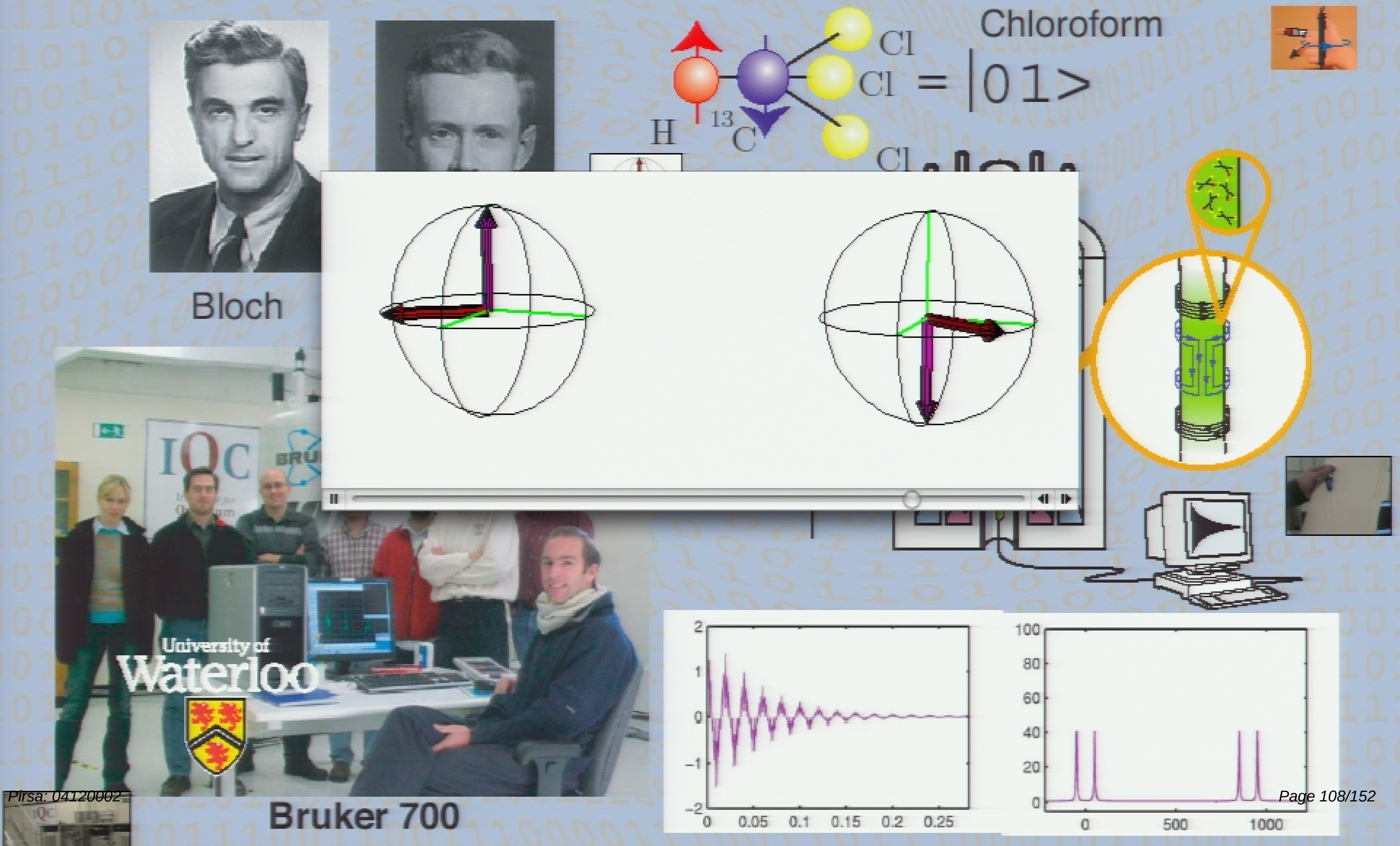
Nuclear Magnetic Resonance



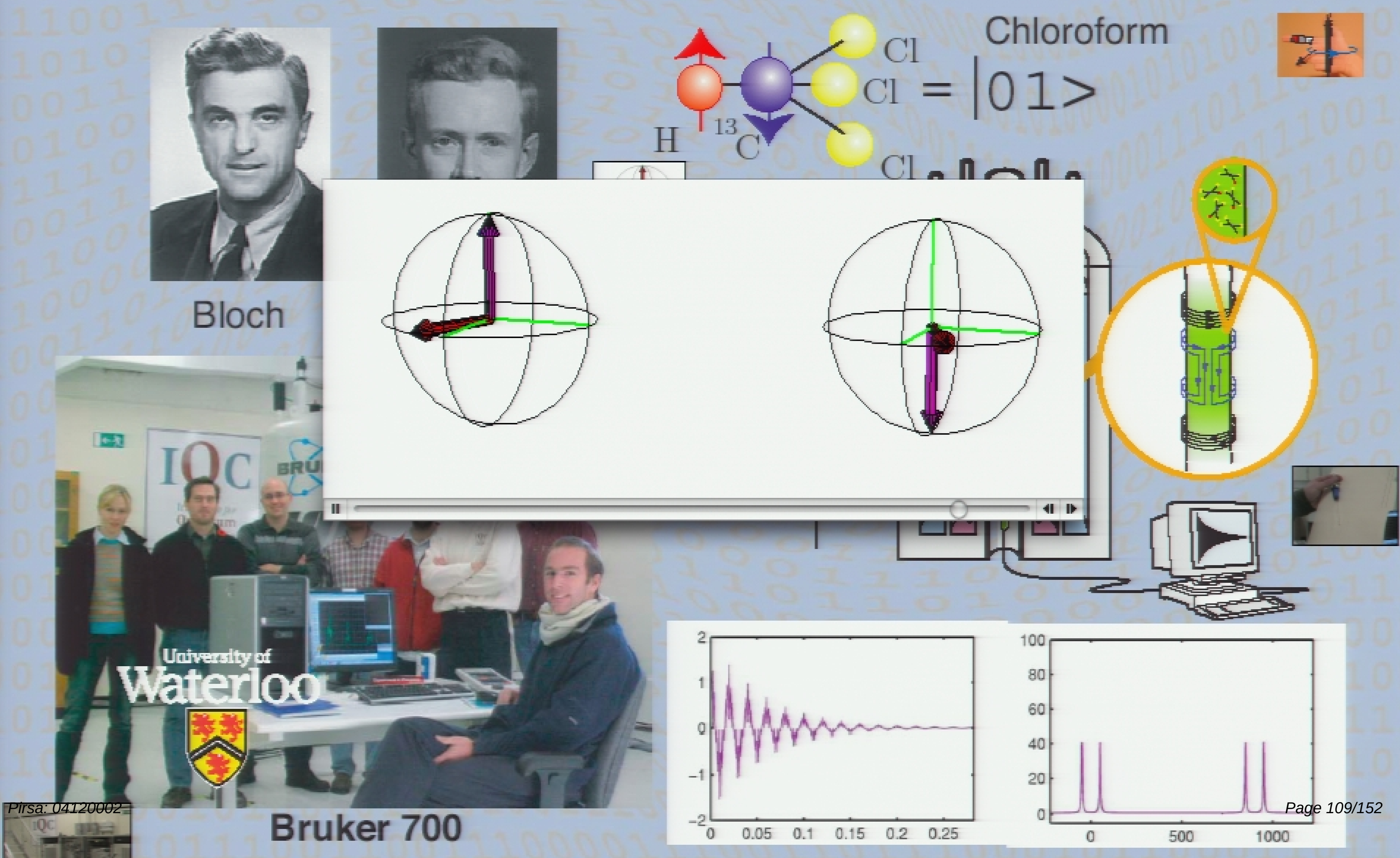
Nuclear Magnetic Resonance



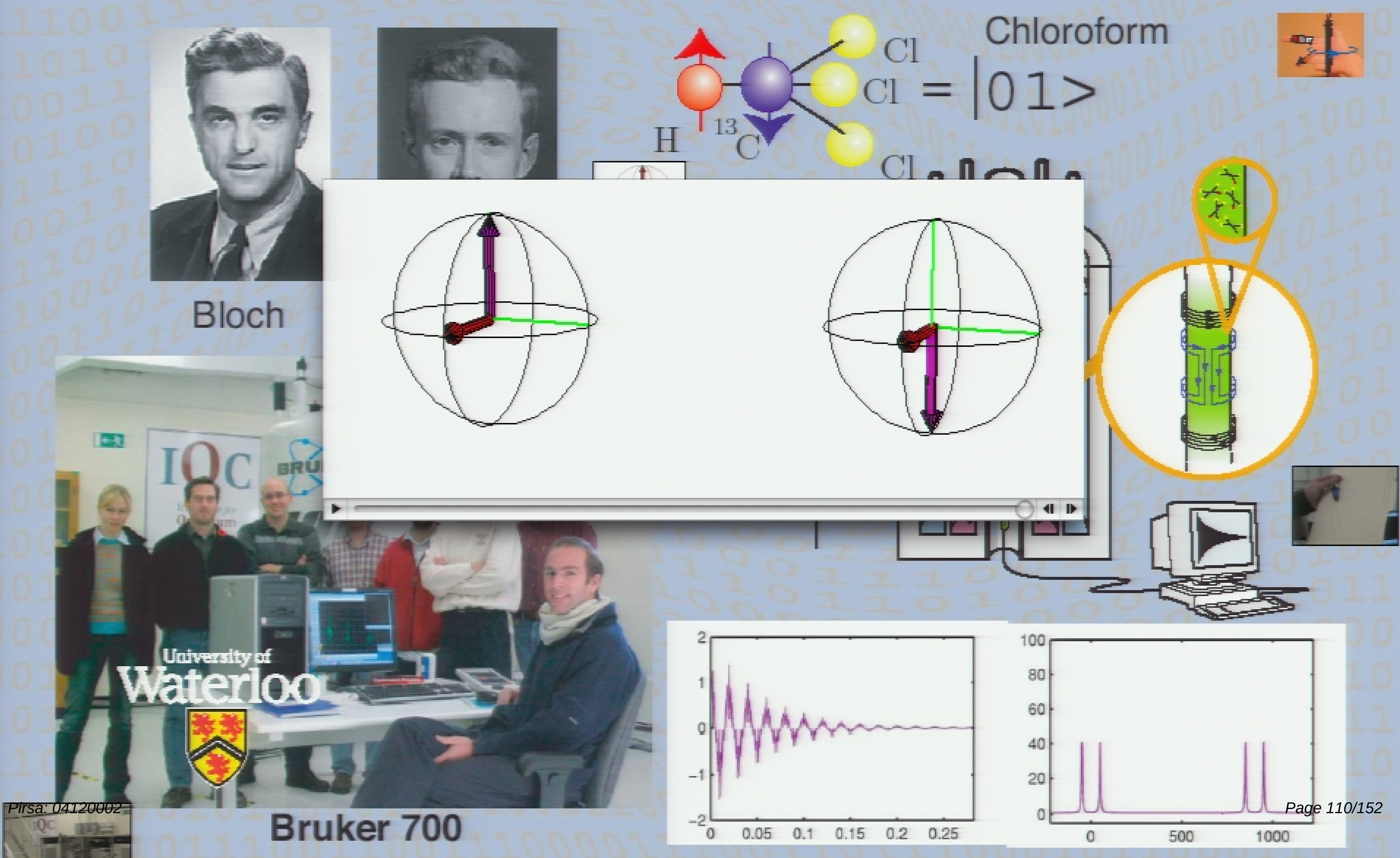
Nuclear Magnetic Resonance



Nuclear Magnetic Resonance

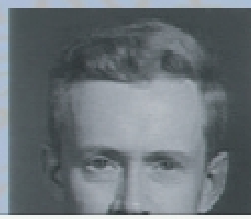


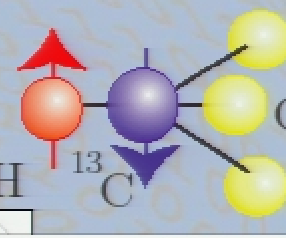
Nuclear Magnetic Resonance



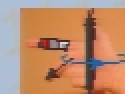
Nuclear Magnetic Resonance

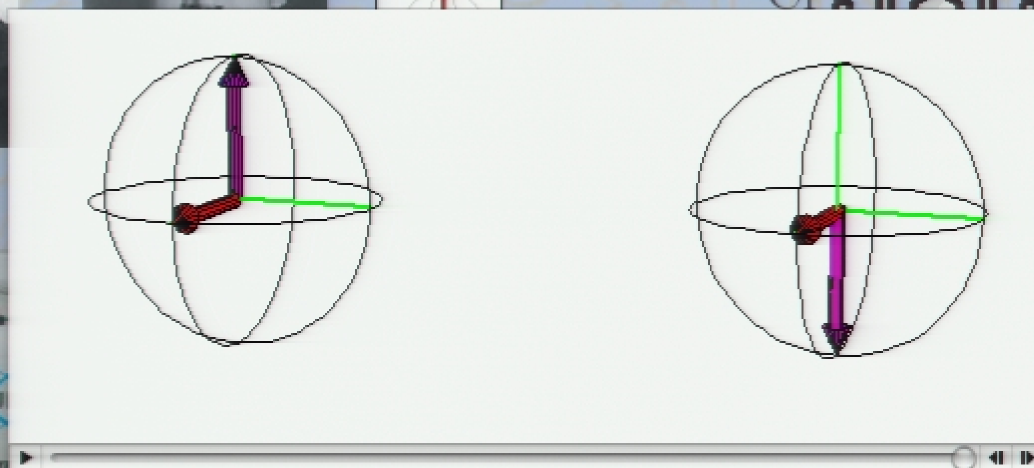
Bloch

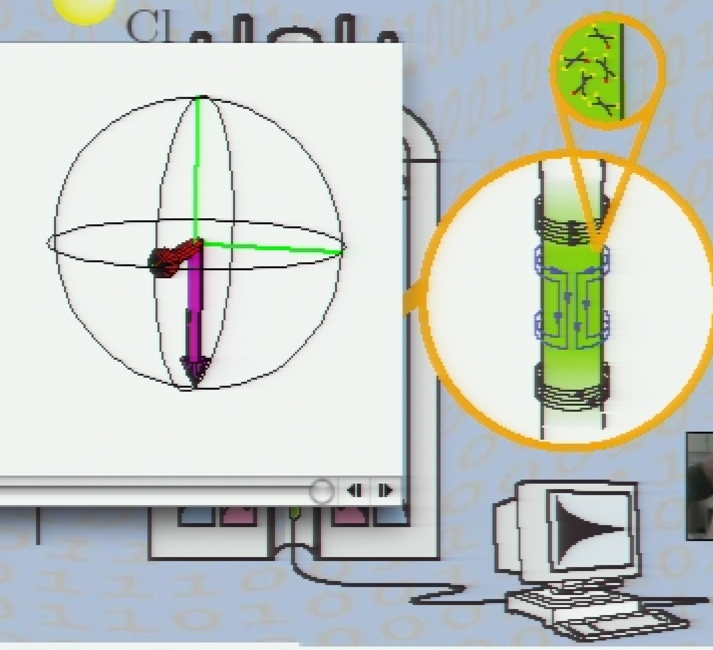


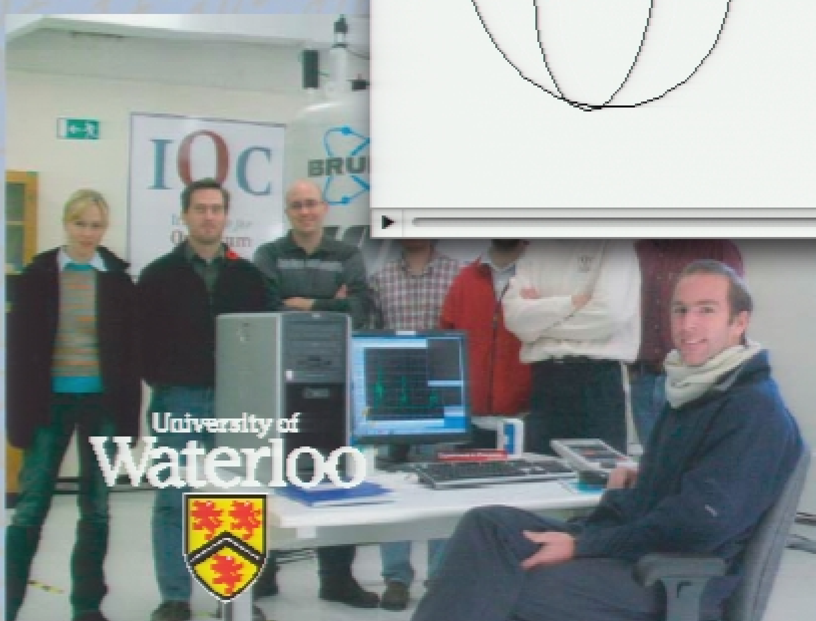


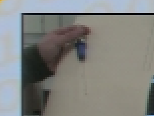
Chloroform $= |01>$

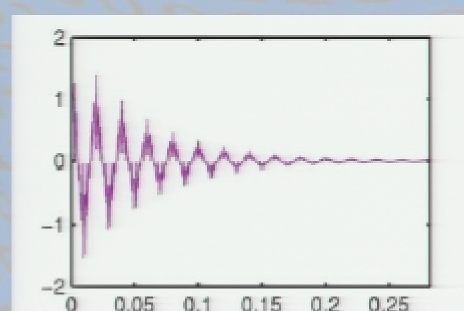


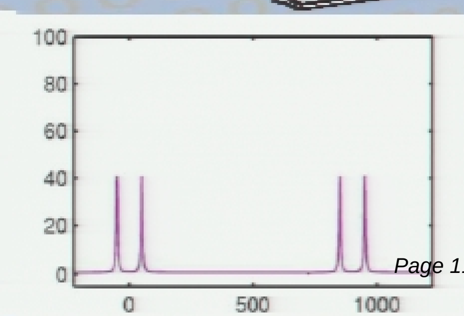






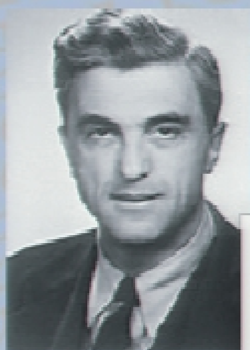




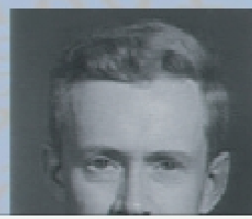


Bruker 700

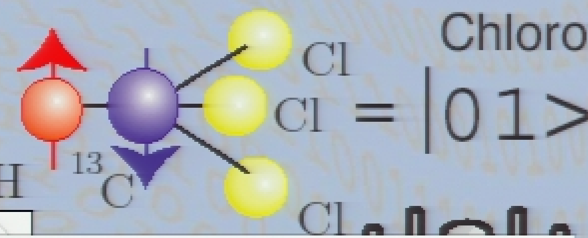
Nuclear Magnetic Resonance

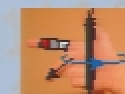


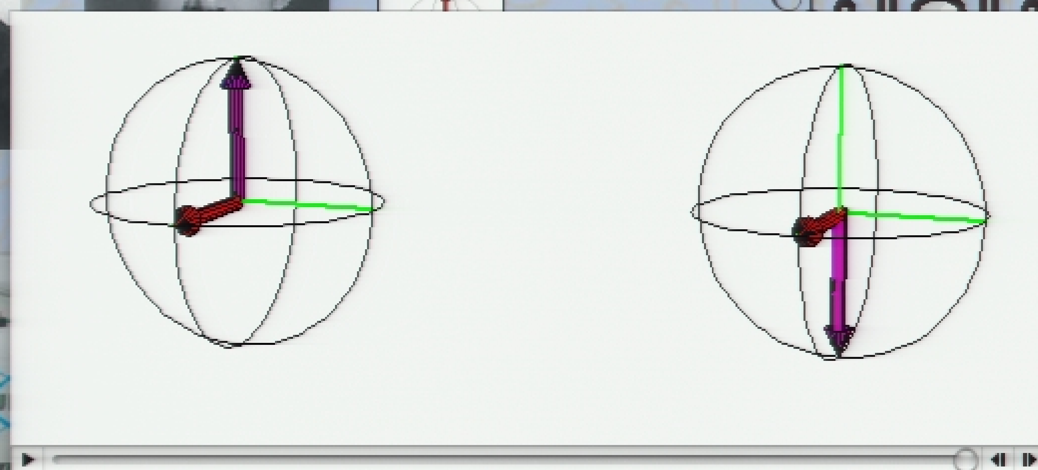
Bloch

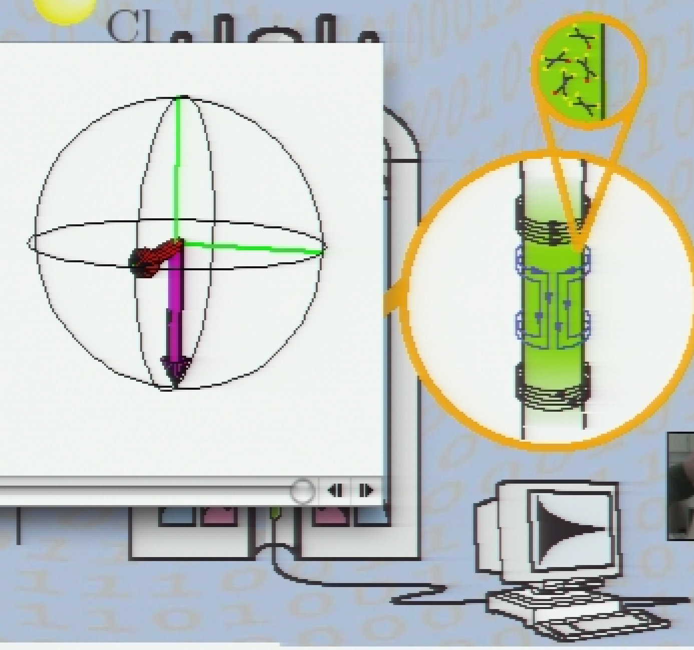


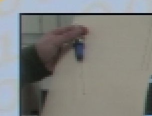
Chloroform

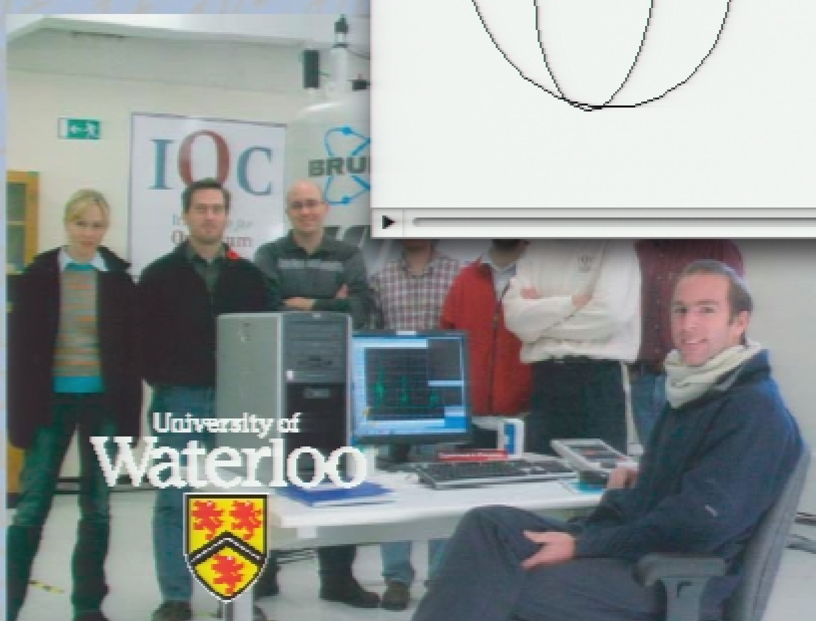




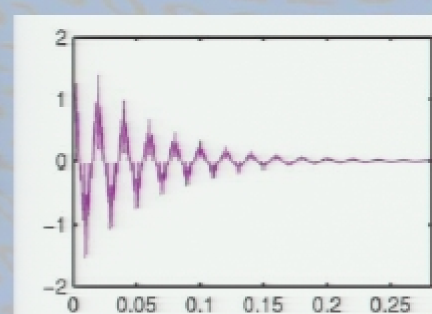


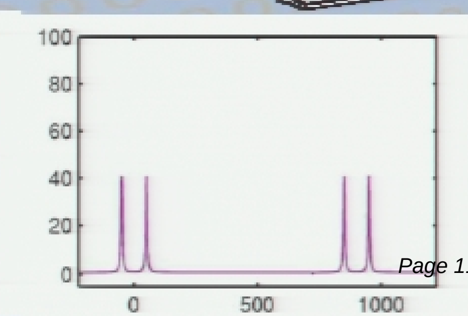


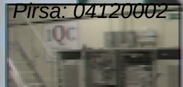




Bruker 700



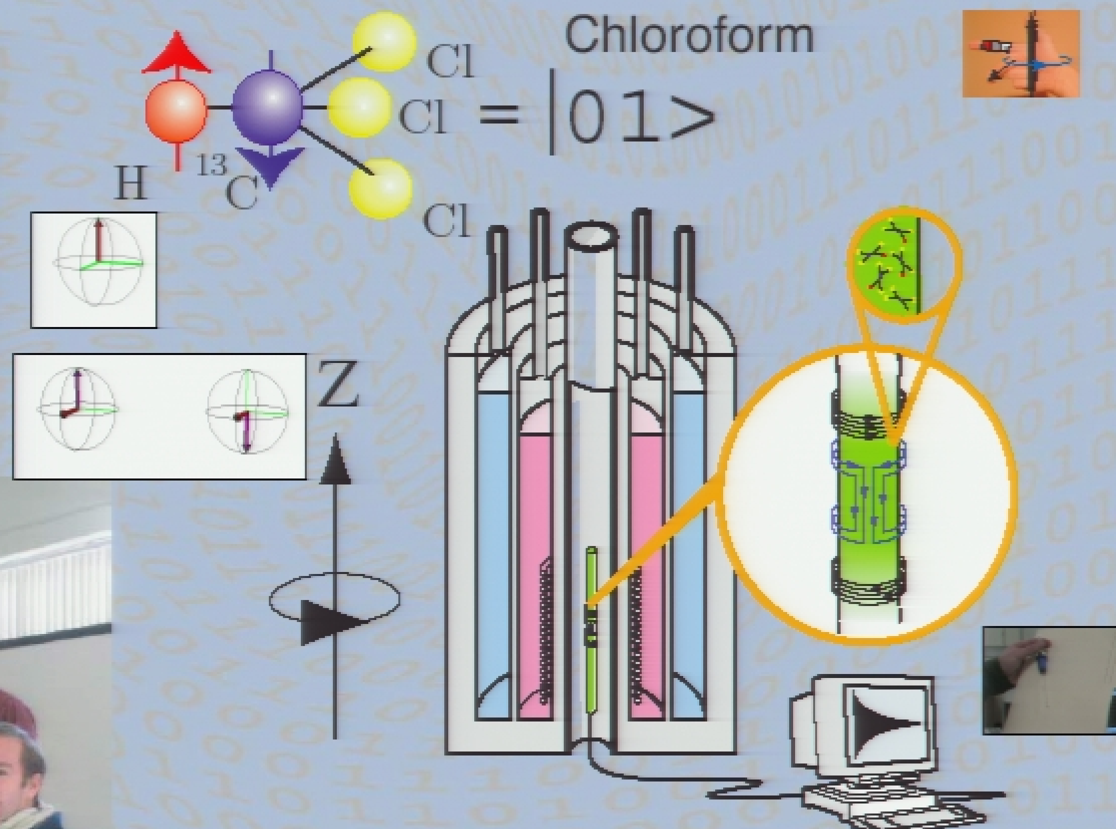




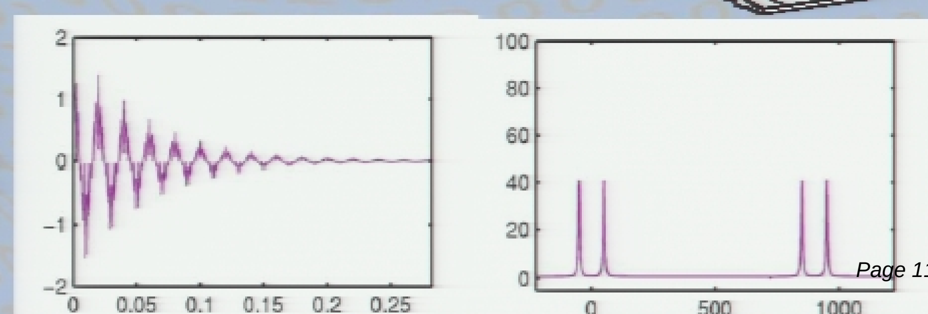
Nuclear Magnetic Resonance

Bloch

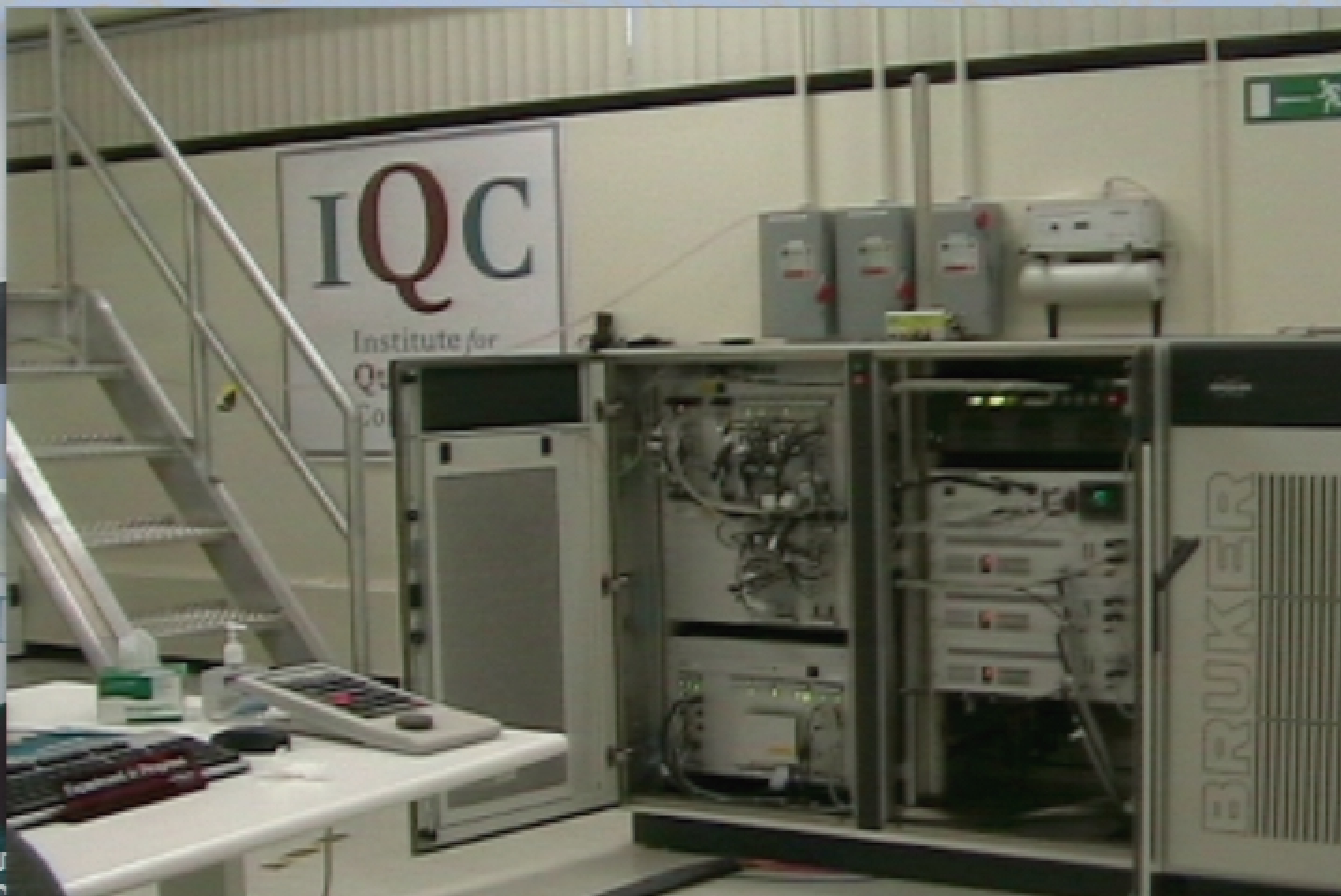
Purcell

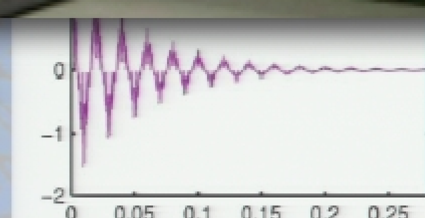


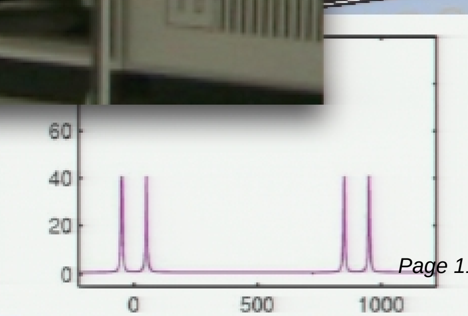
Bruker 700



Nuclear Magnetic Resonance

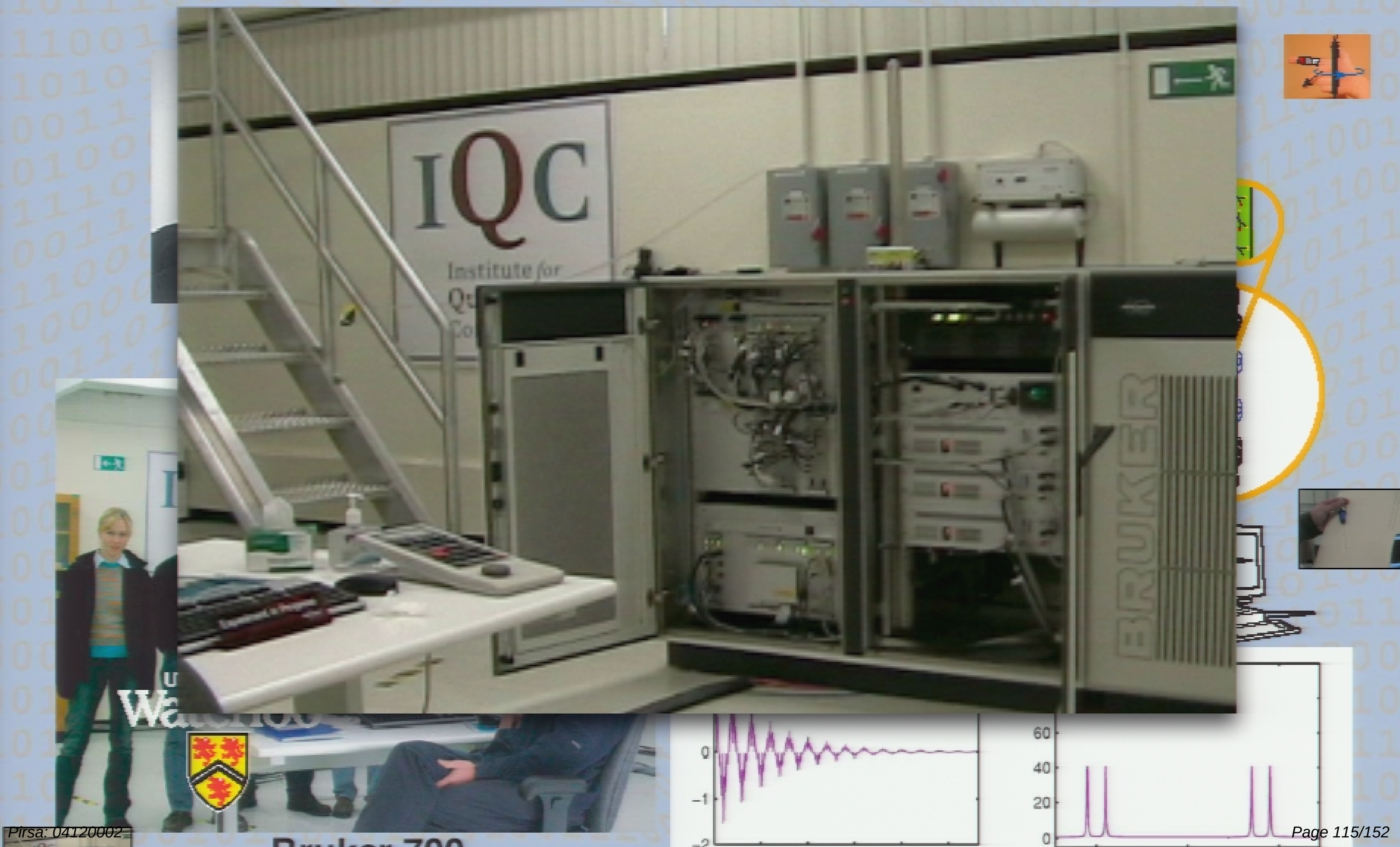






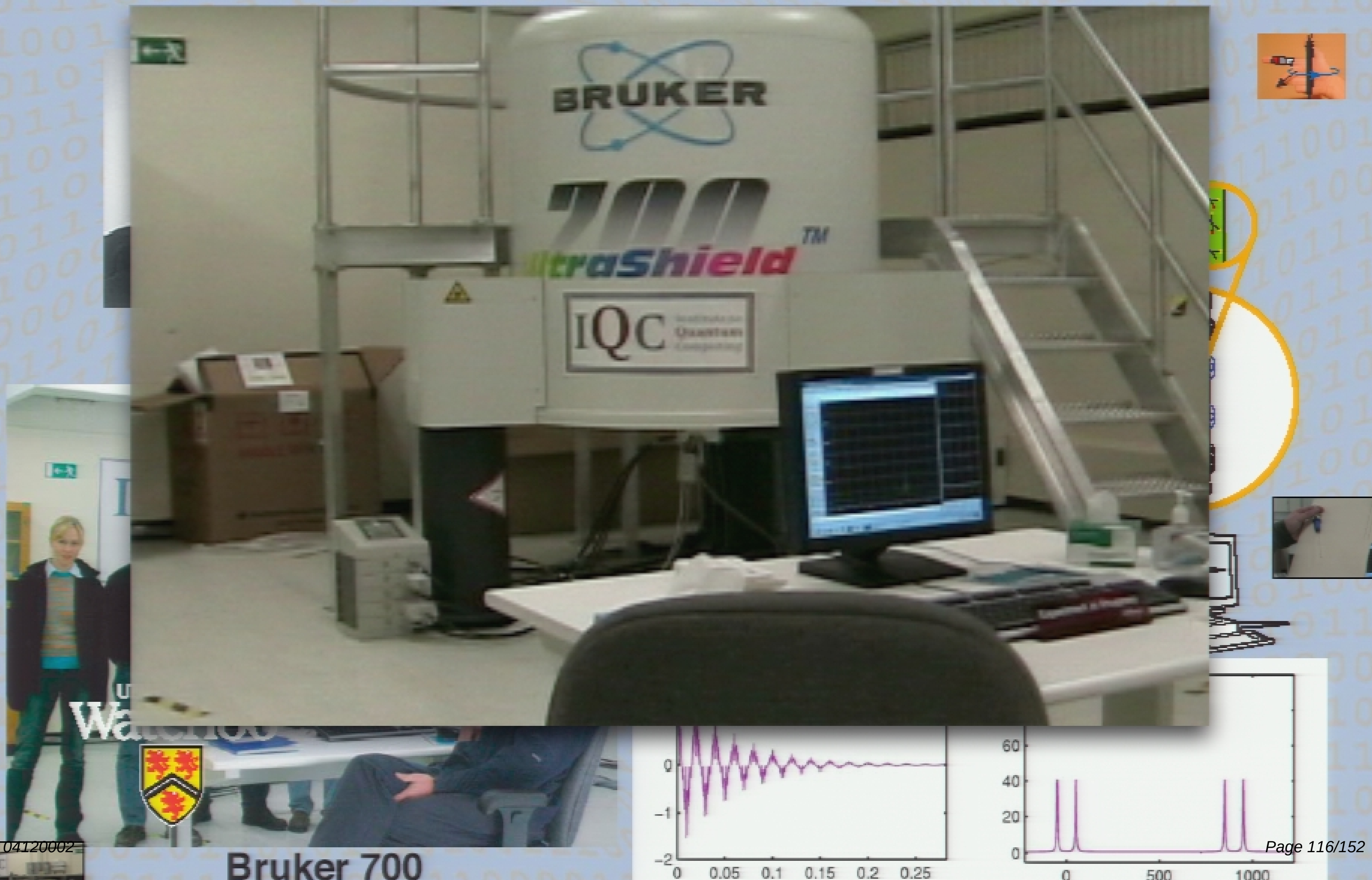
Bruker 700

Nuclear Magnetic Resonance



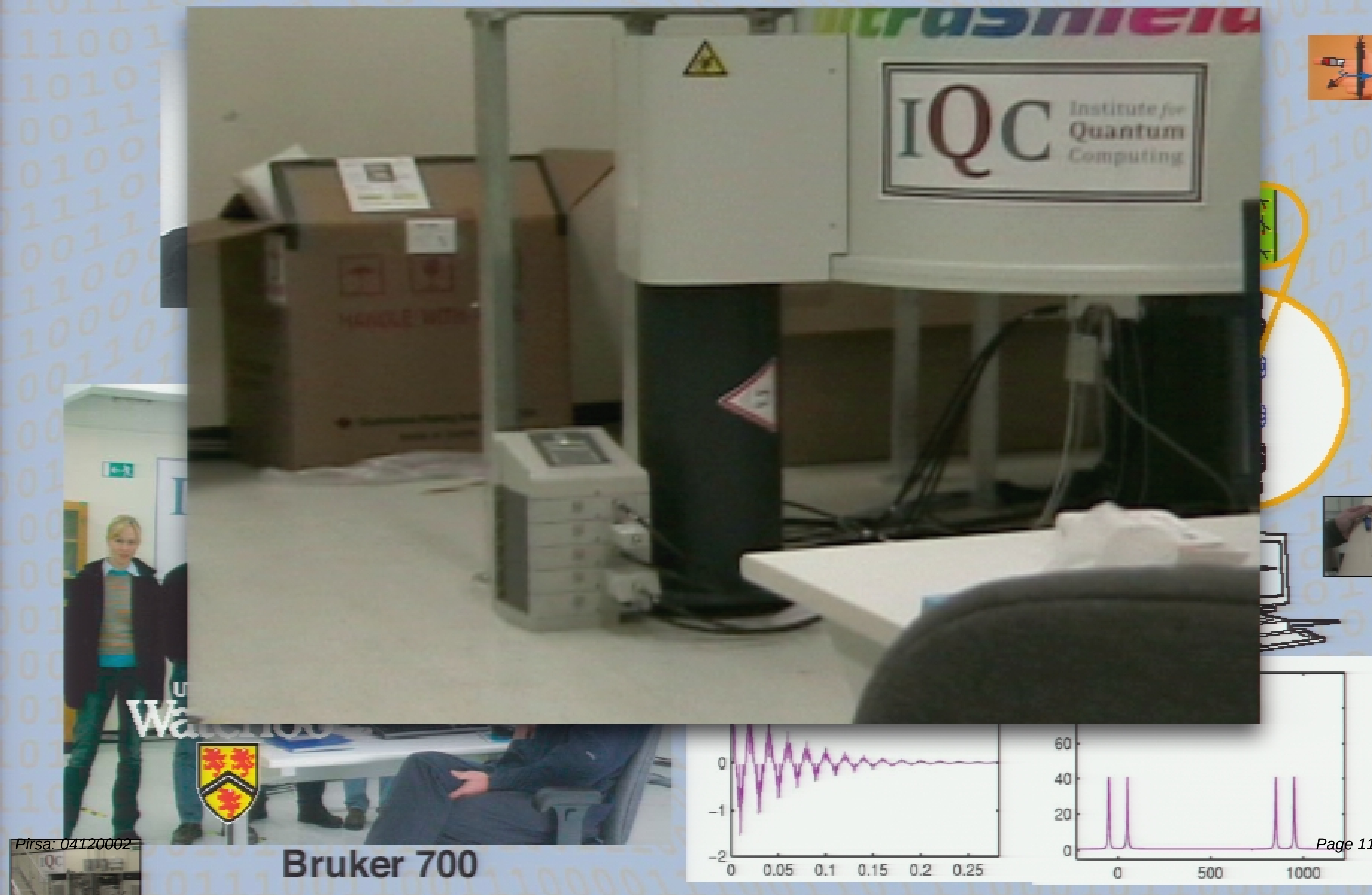
Bruker 700

Nuclear Magnetic Resonance

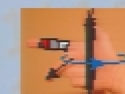


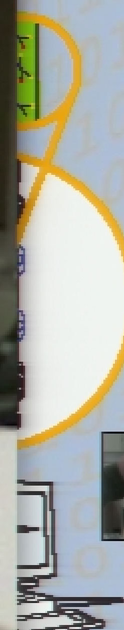
Bruker 700

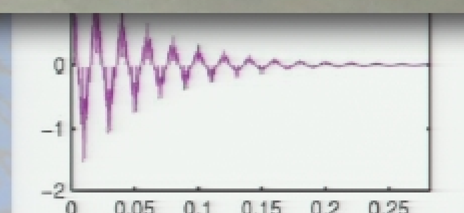
Nuclear Magnetic Resonance

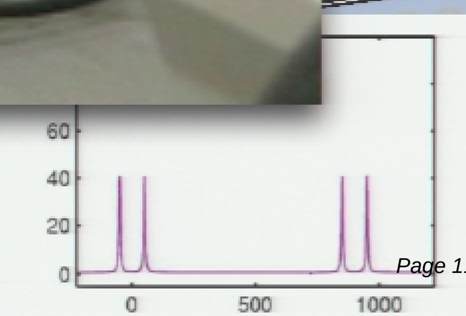


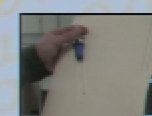
Nuclear Magnetic Resonance

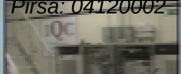






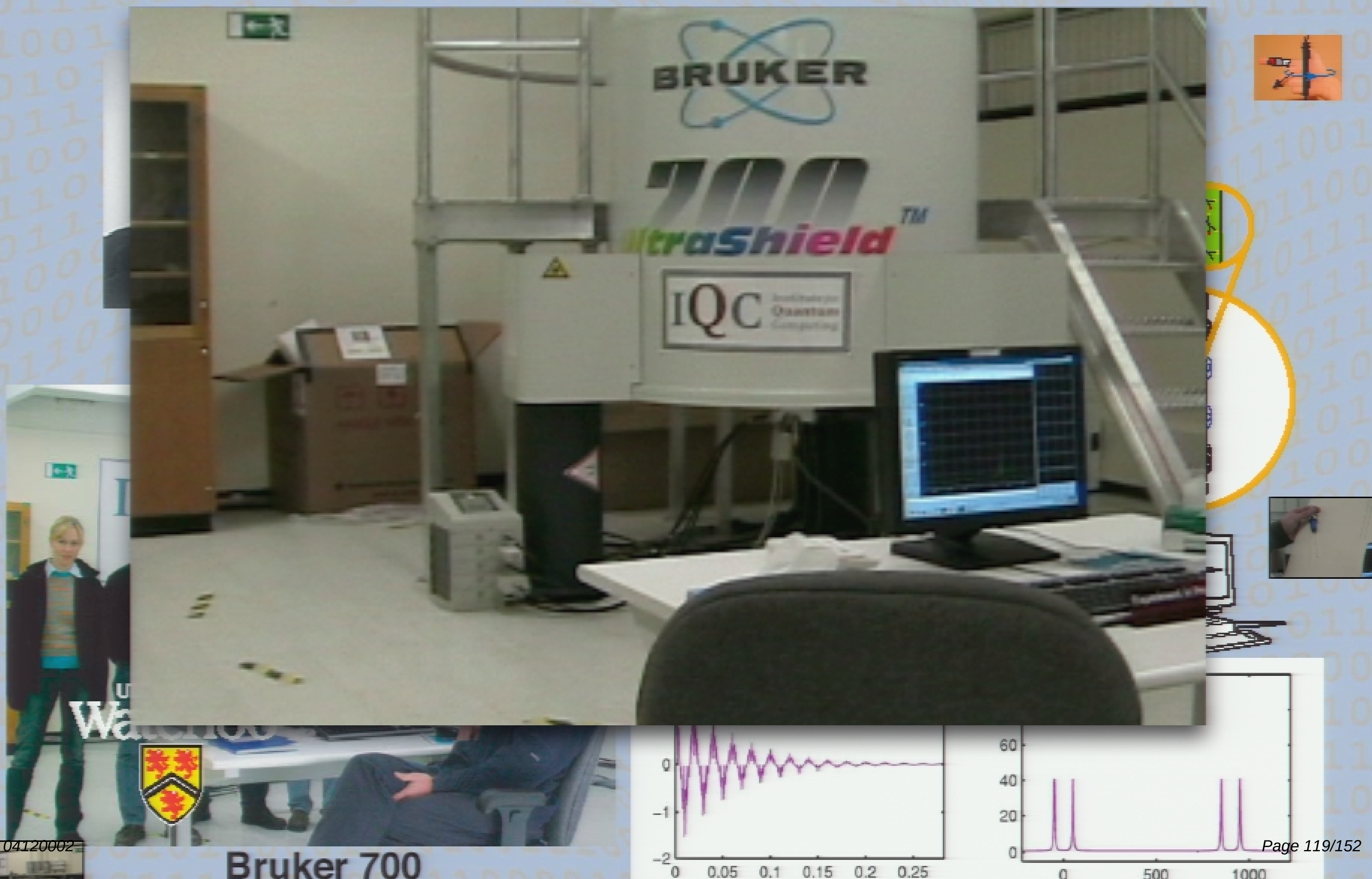






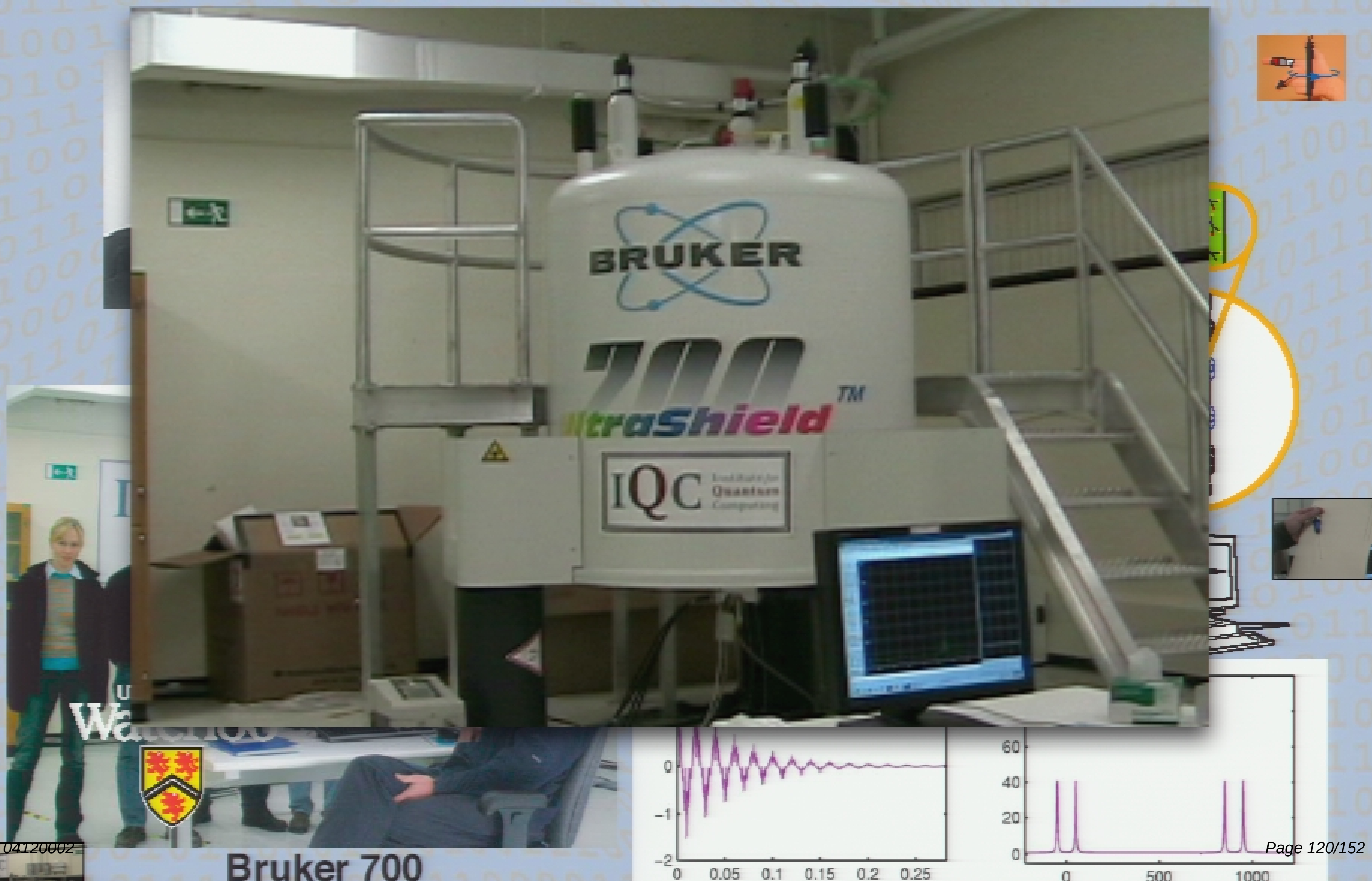
Bruker 700

Nuclear Magnetic Resonance



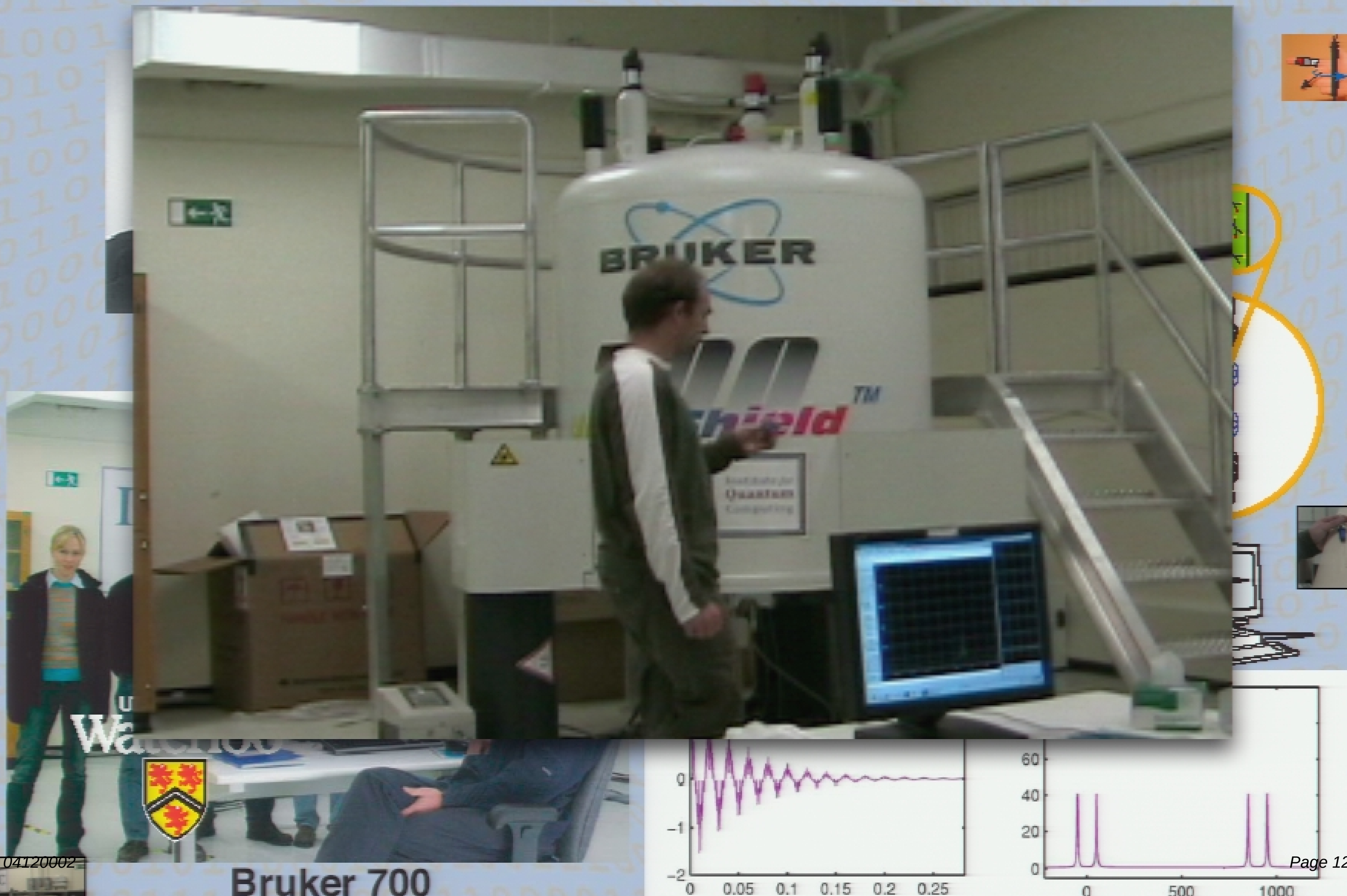
Bruker 700

Nuclear Magnetic Resonance



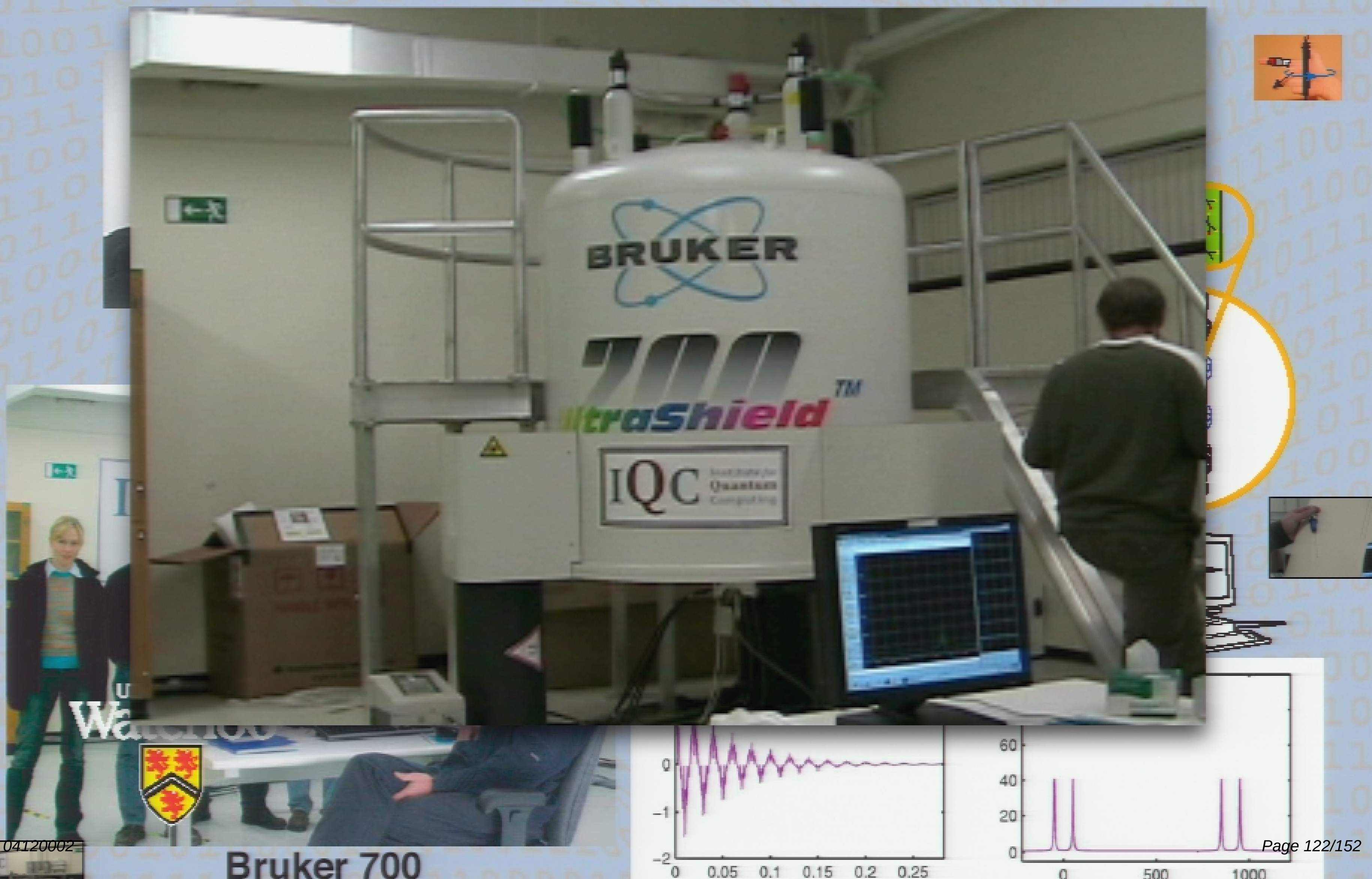
Bruker 700

Nuclear Magnetic Resonance



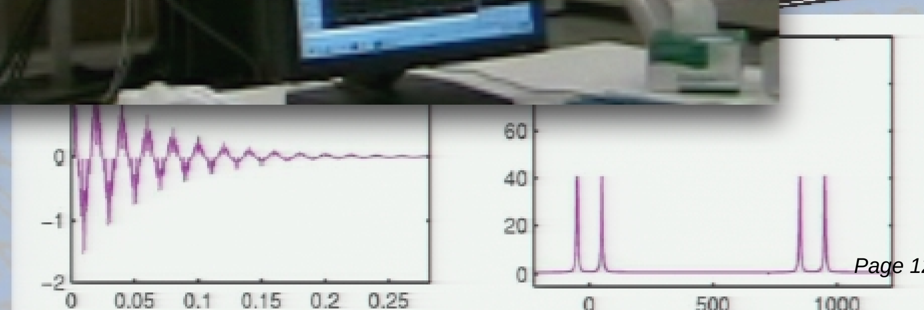
Bruker 700

Nuclear Magnetic Resonance



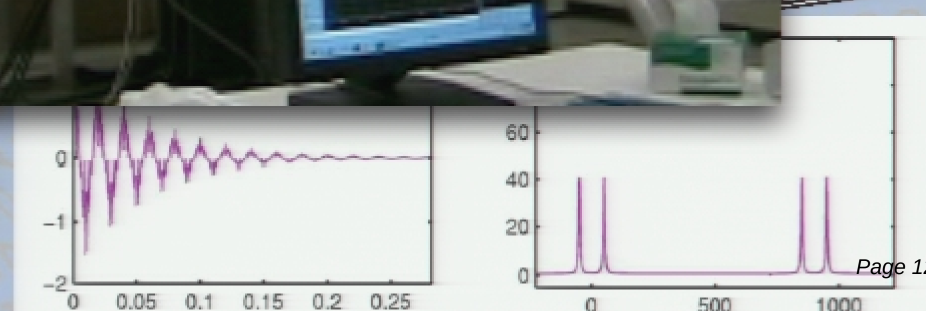
Bruker 700

Nuclear Magnetic Resonance



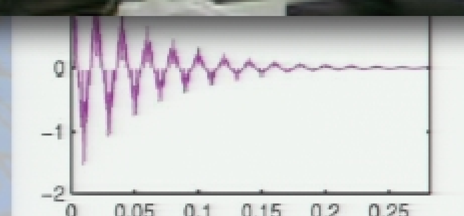
Bruker 700

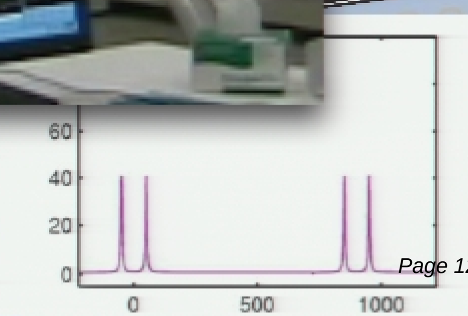
Nuclear Magnetic Resonance



Bruker 700

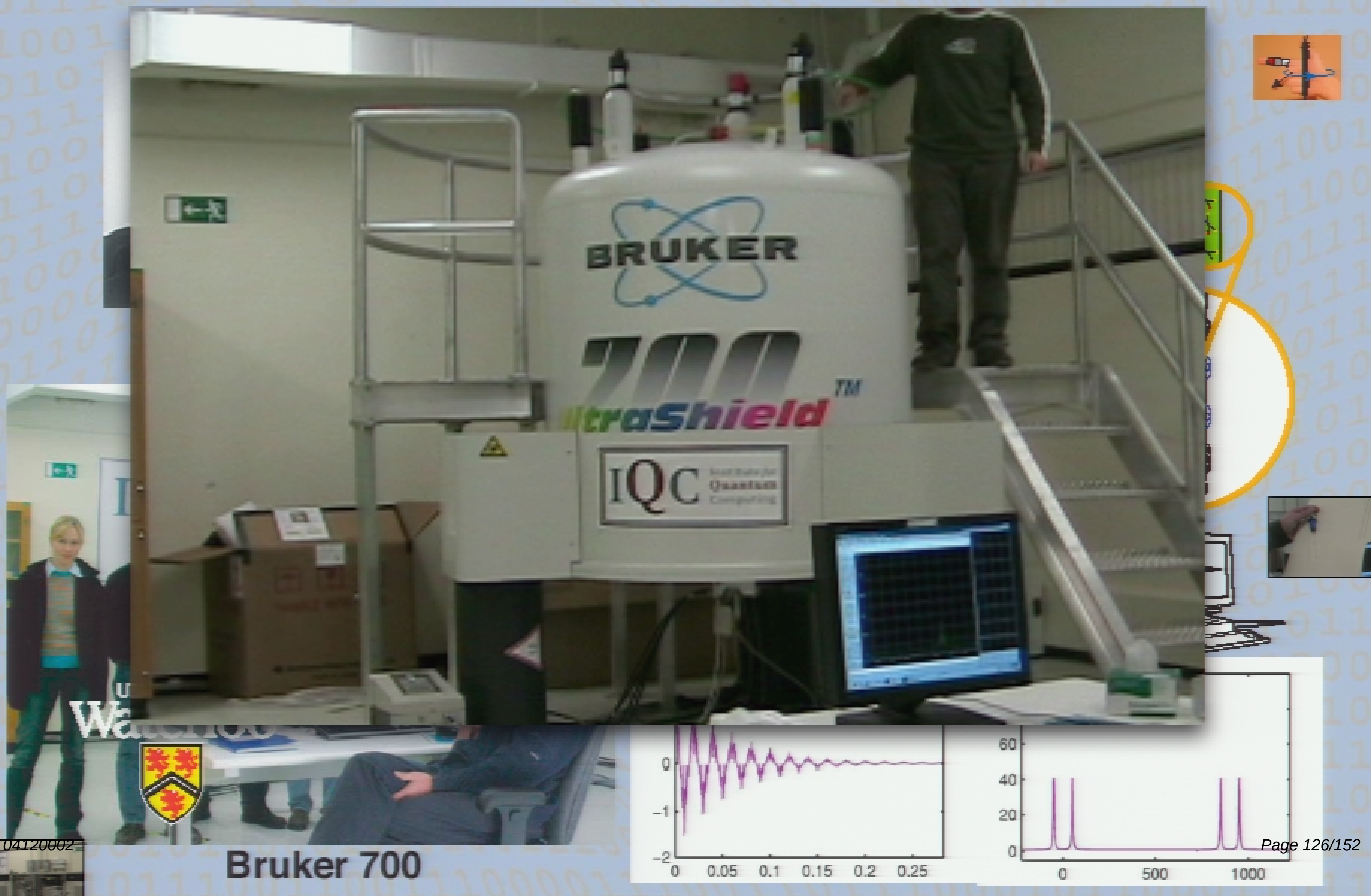
Nuclear Magnetic Resonance





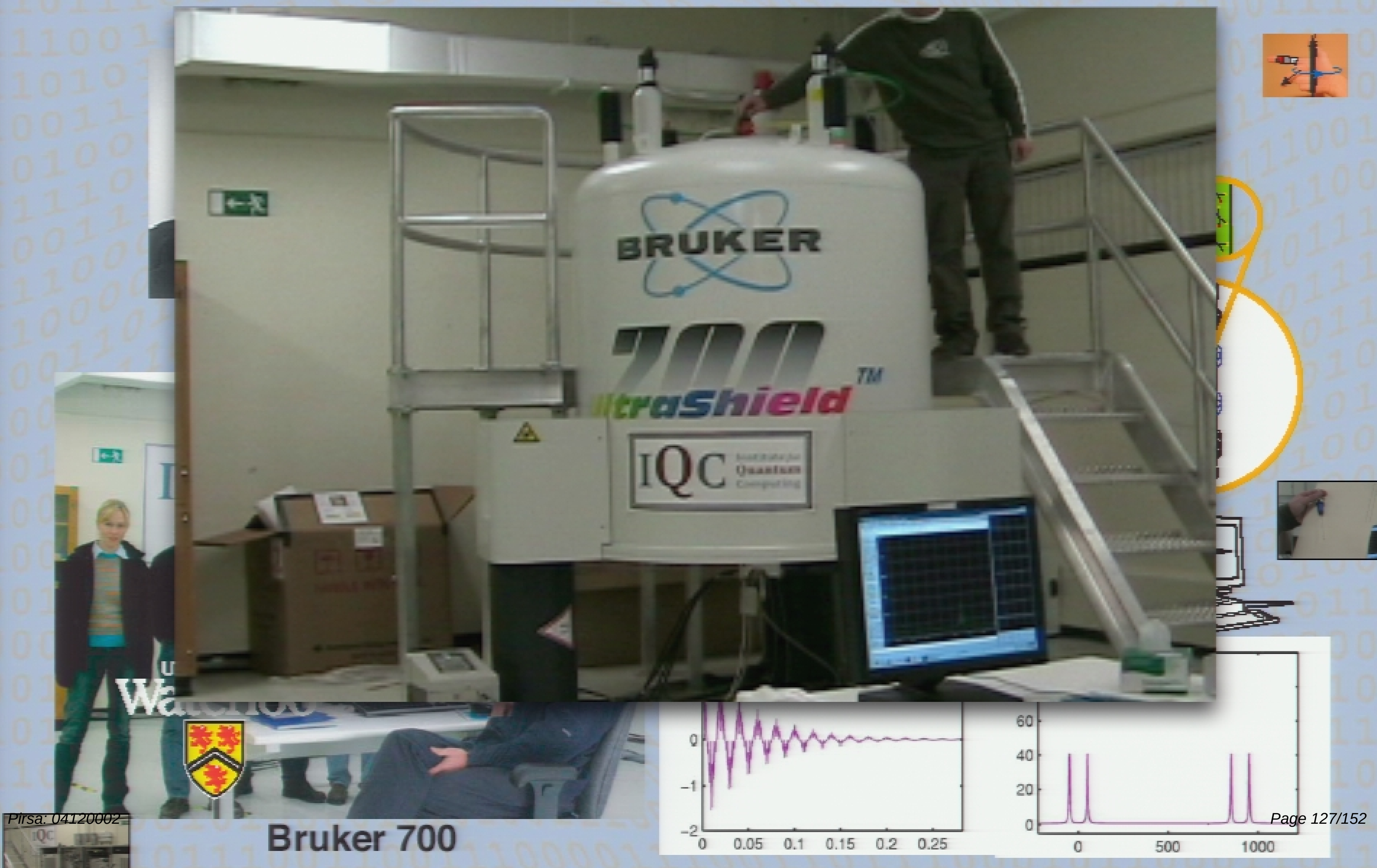
Bruker 700

Nuclear Magnetic Resonance



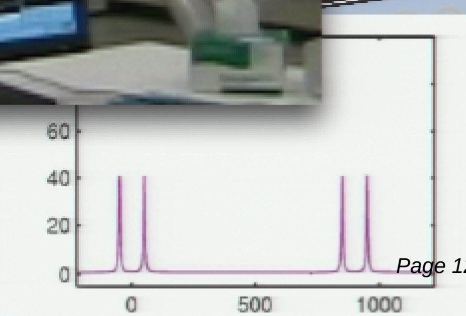
Bruker 700

Nuclear Magnetic Resonance



Bruker 700

Nuclear Magnetic Resonance

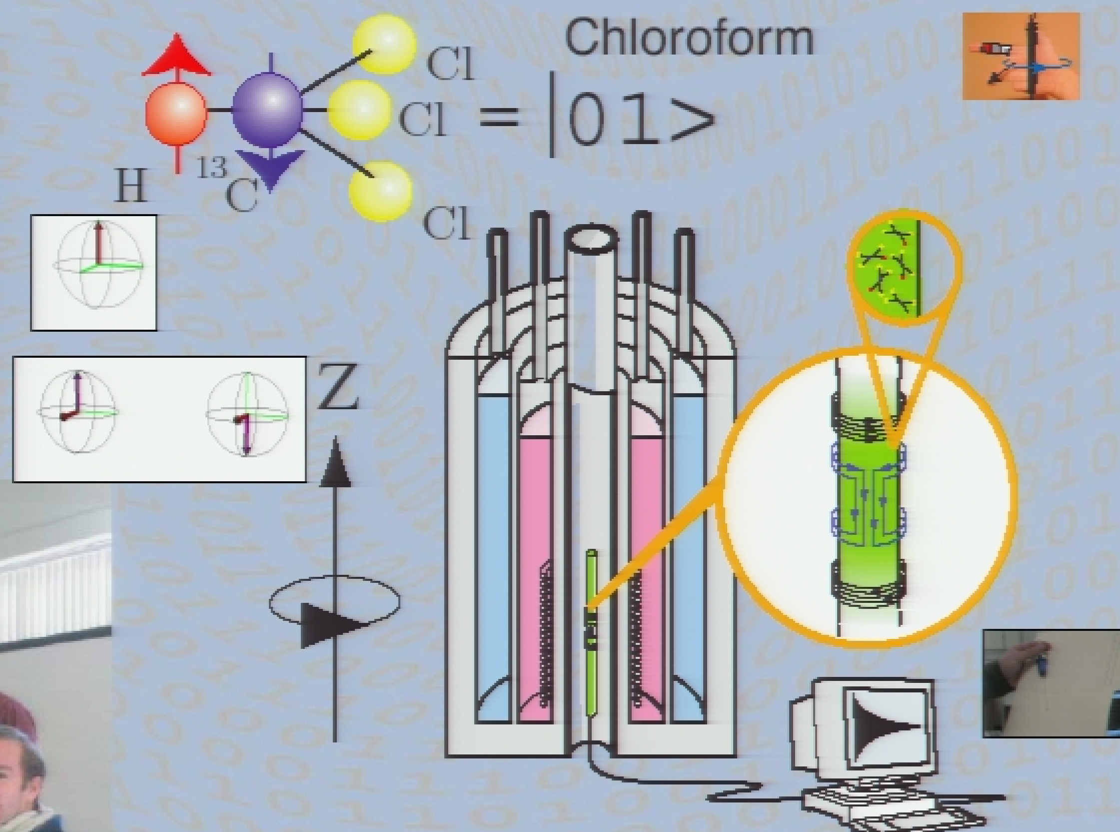


Bruker 700

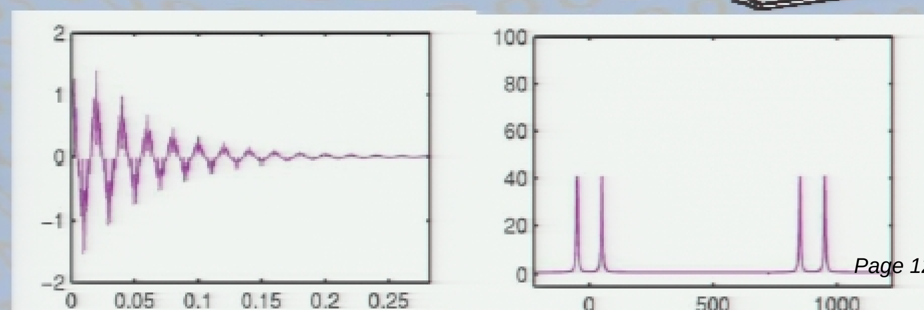
Nuclear Magnetic Resonance

Bloch

Purcell

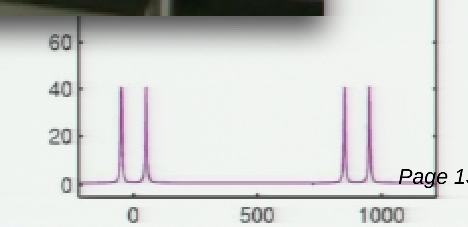


Bruker 700



Nuclear Magnetic Resonance

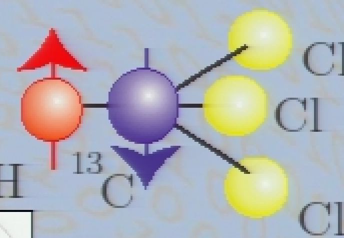
Bruker 700



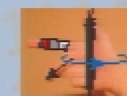
Nuclear Magnetic Resonance

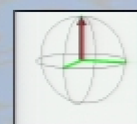
Bloch

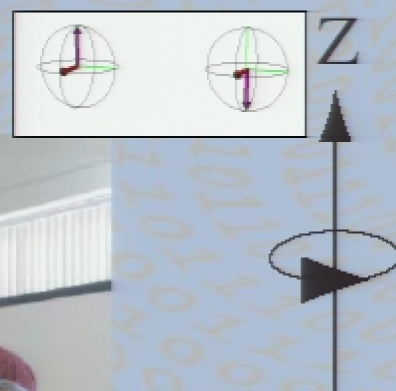
Purcell

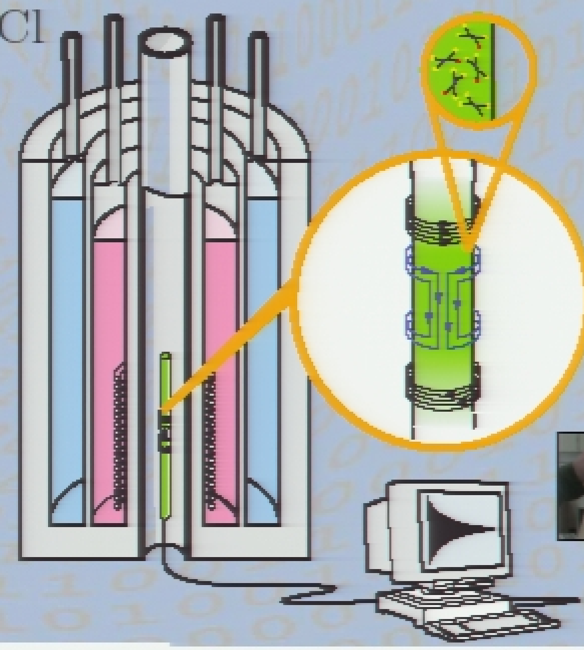


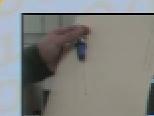
Chloroform $= |01\rangle$

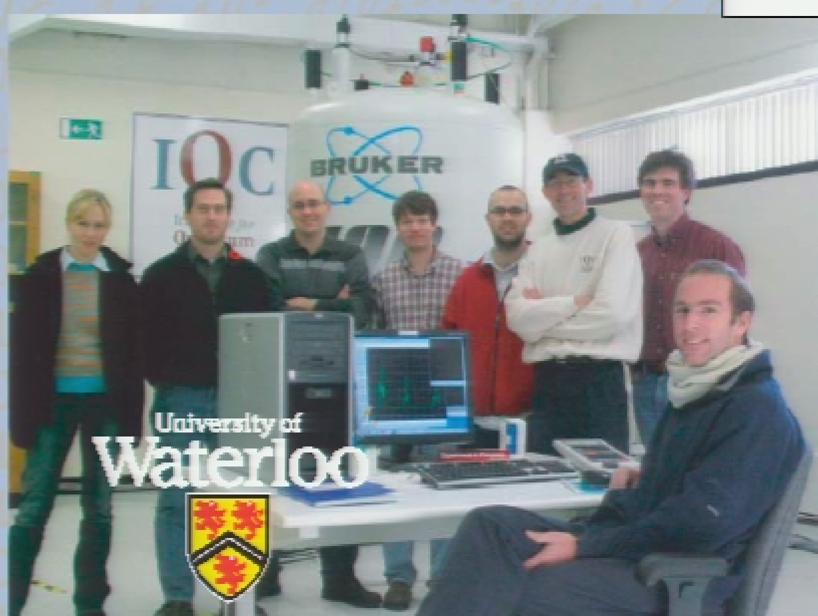




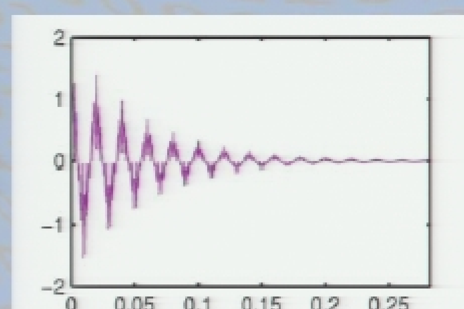


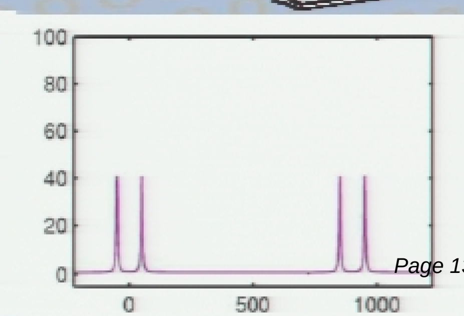






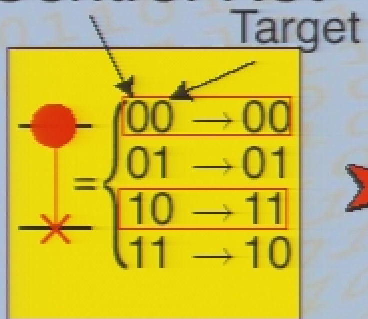
Bruker 700



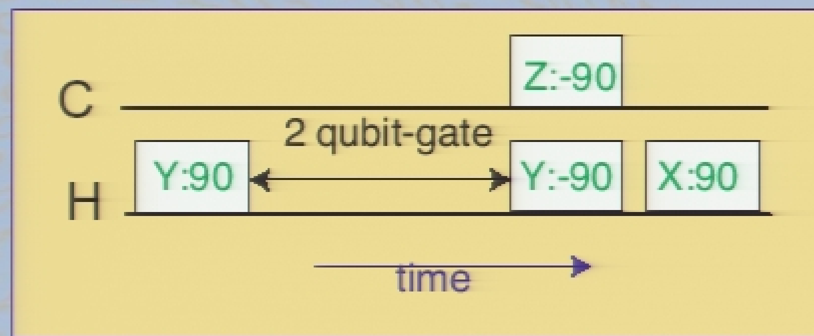


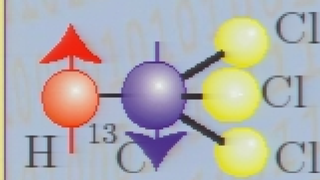
Quantum algorithms 101: the Control-NOT

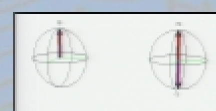
Control-Not



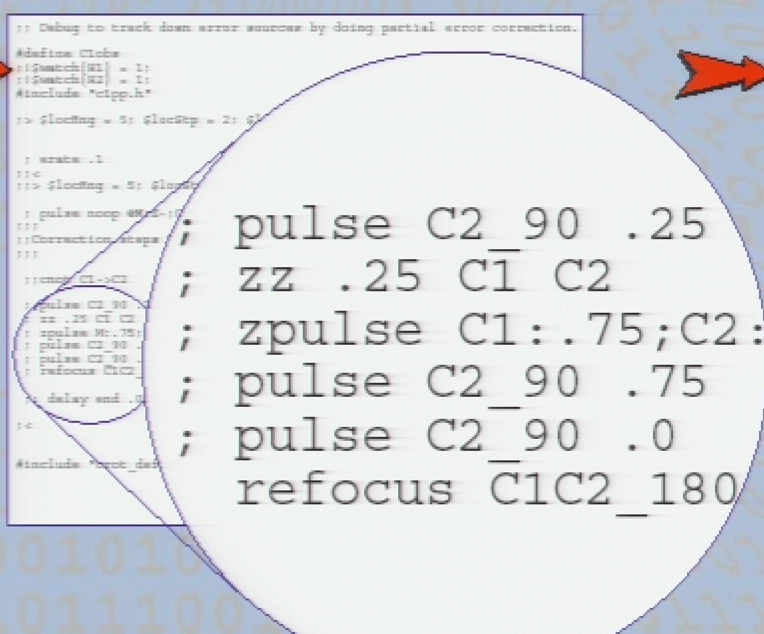
Quantum circuit



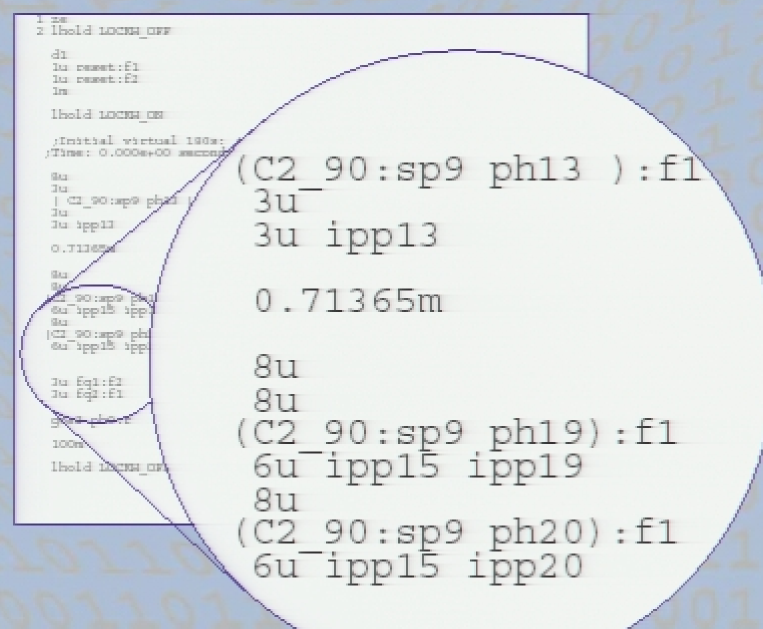




Pre-compiler (Optimizer)

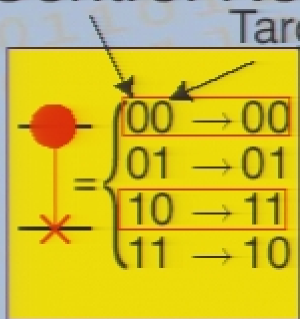


Bruker (machine) language

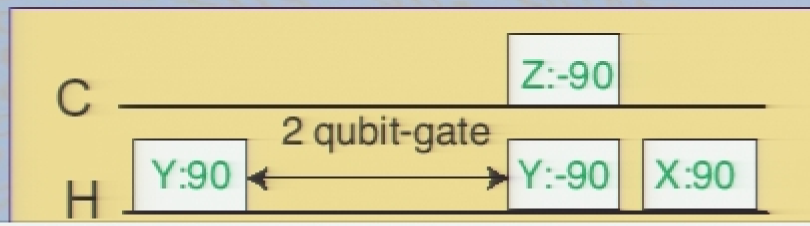


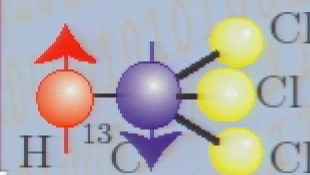
Quantum algorithms 101: the Control-NOT

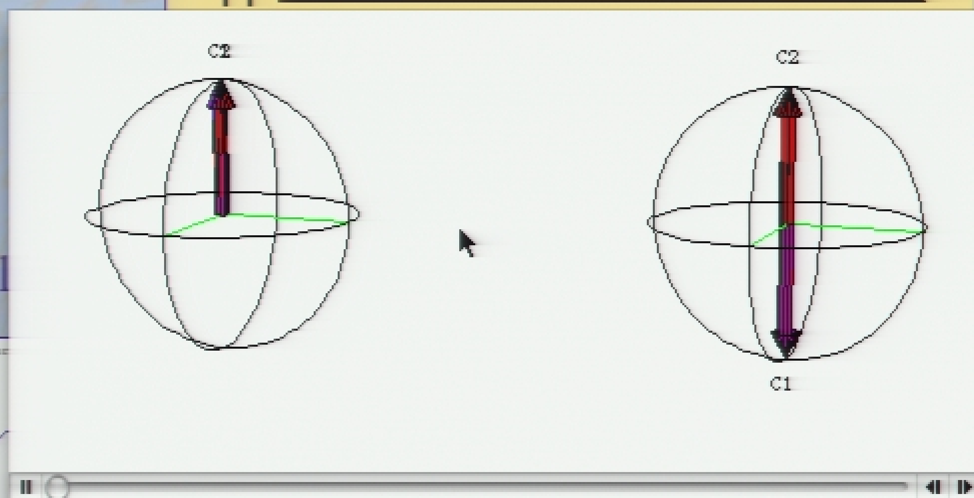
Control-Not



Quantum circuit





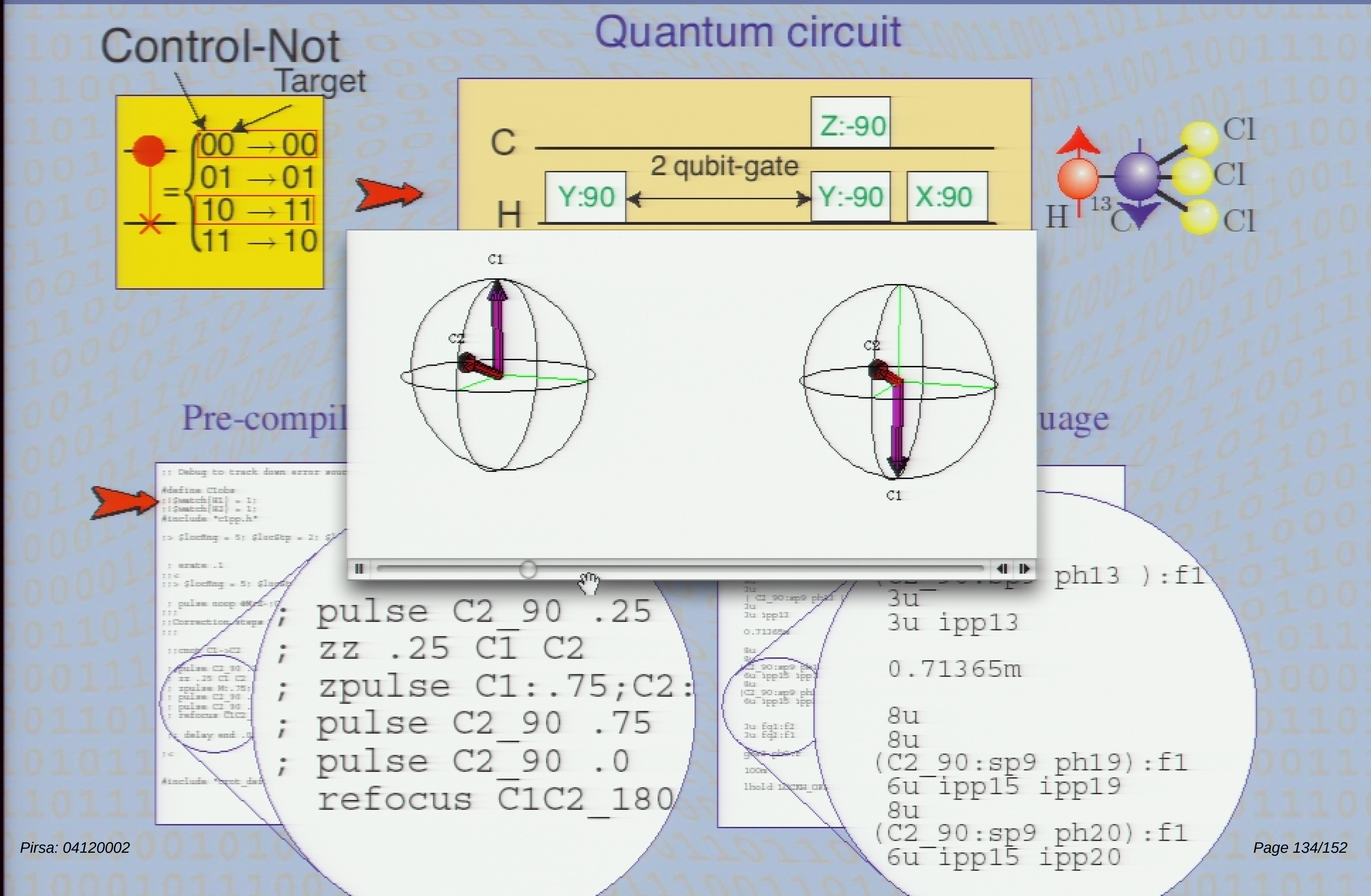


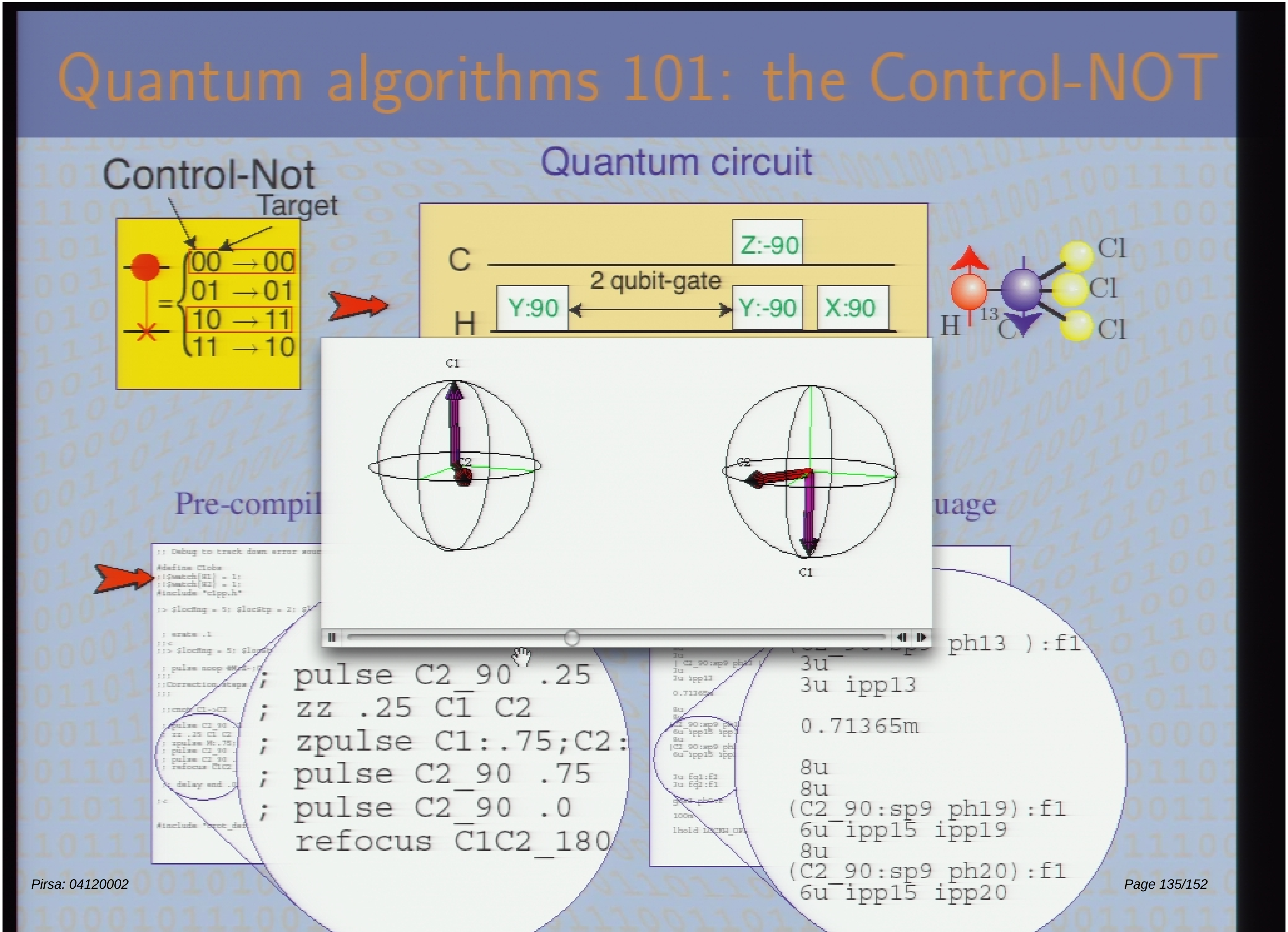
Pre-compil… …uage

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

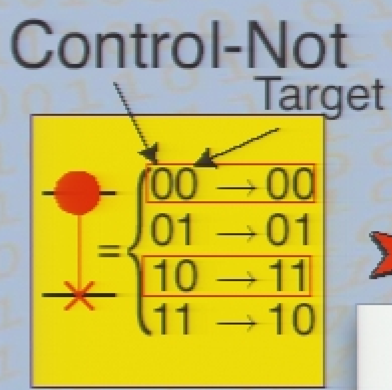
```
(C2_90:sp9 ph13 ):f1
3u
3u ipp13

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

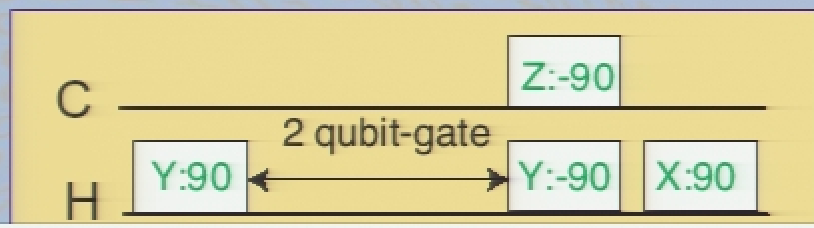


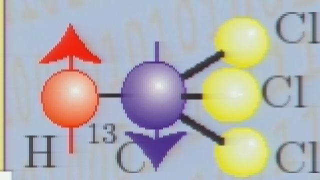

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
Cl
Cl
Cl
H
13C
C1
C2
C2
C1
Pre-compil
uage
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
ph13):f1
3u
3u ipp13
0.71365m
8u
8u
(C2_90:sp9 ph19):f1
6u ipp15 ipp19
8u
(C2_90:sp9 ph20):f1
6u ipp15 ipp20
Pirsa: 04120002
Page 135/152

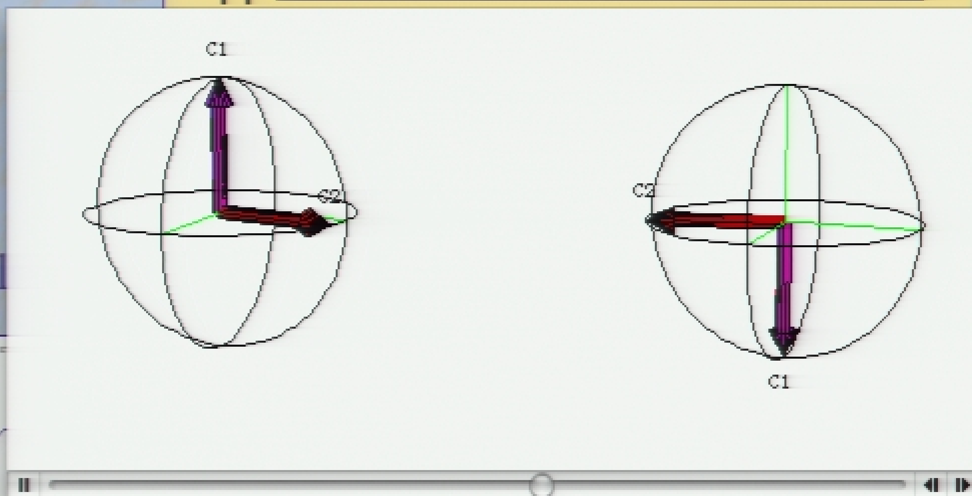
Quantum algorithms 101: the Control-NOT



Quantum circuit





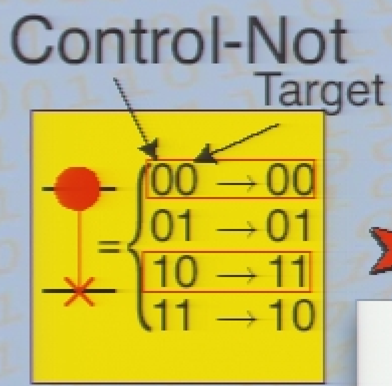


Pre-compil... ...uage

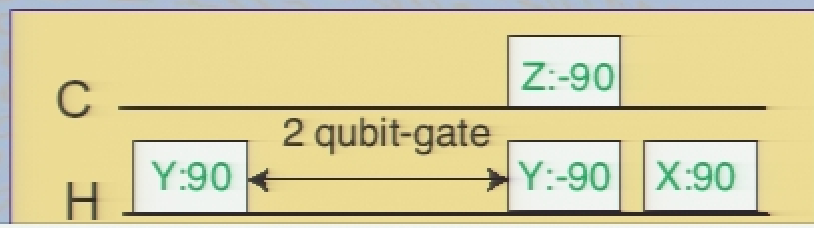
```
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
  refocus C1C2_180
```

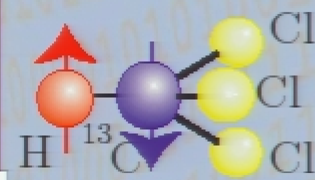
```
(C2_90:sp9 ph13 ):f1
3u
3u ipp13

0.71365m

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

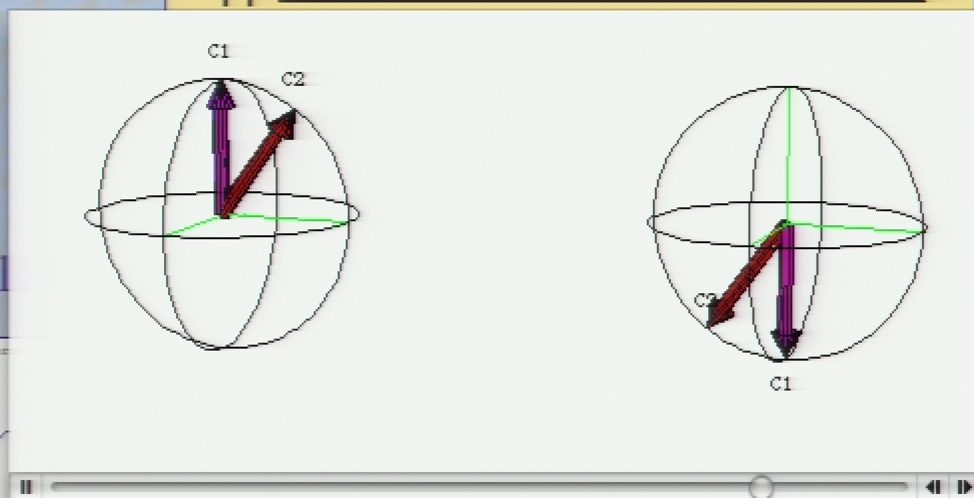
Quantum algorithms 101: the Control-NOT



Quantum circuit



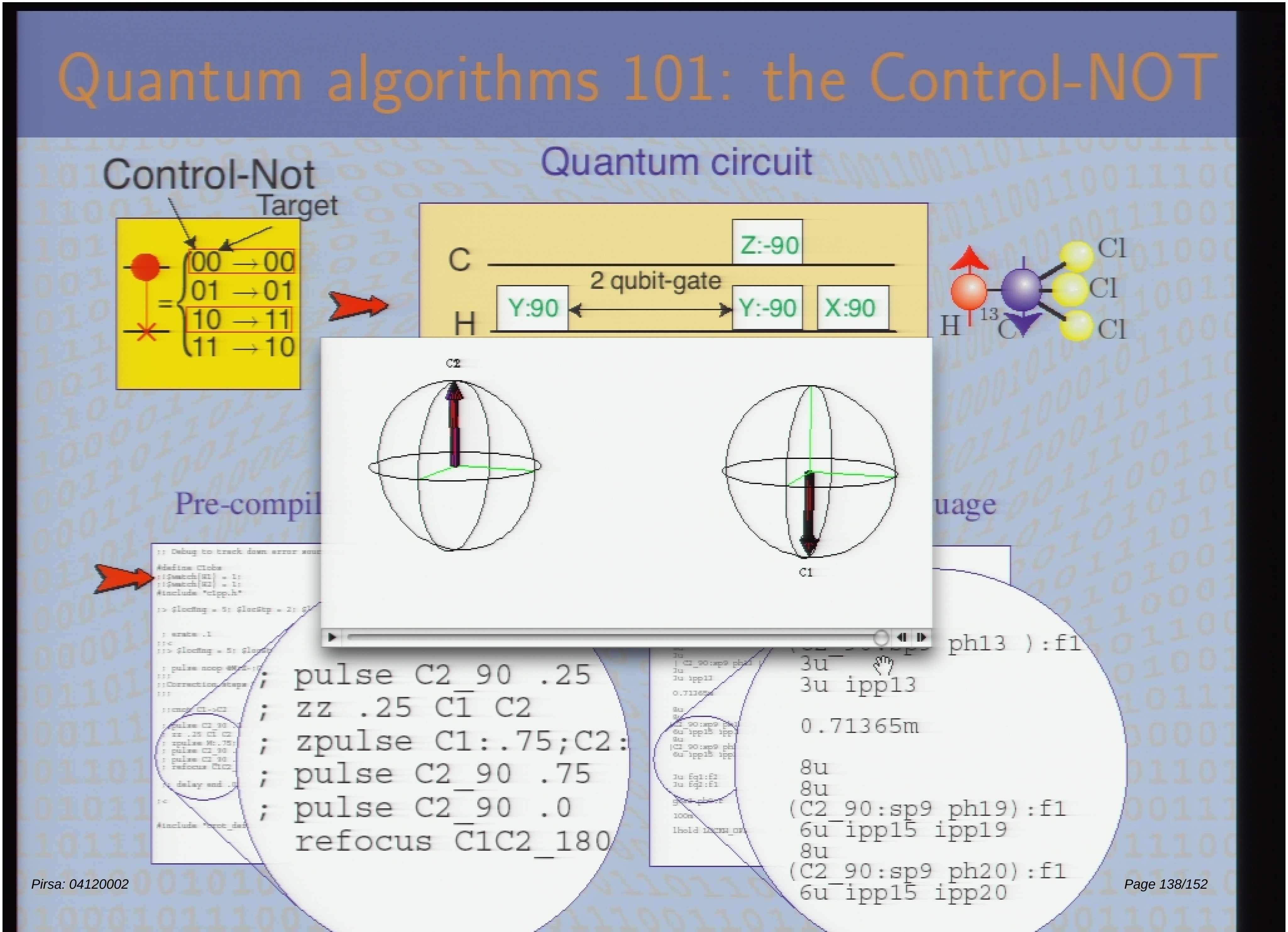


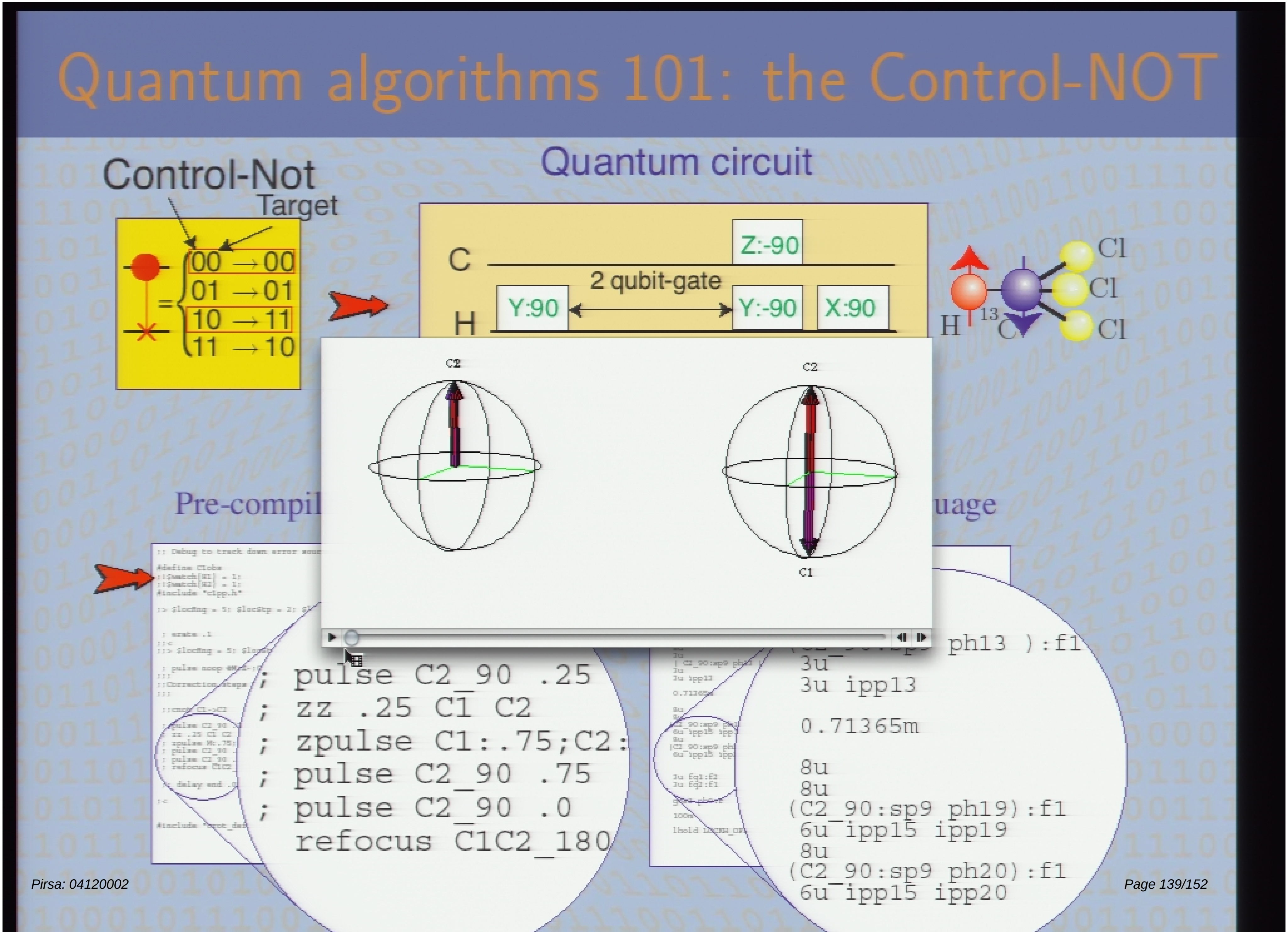


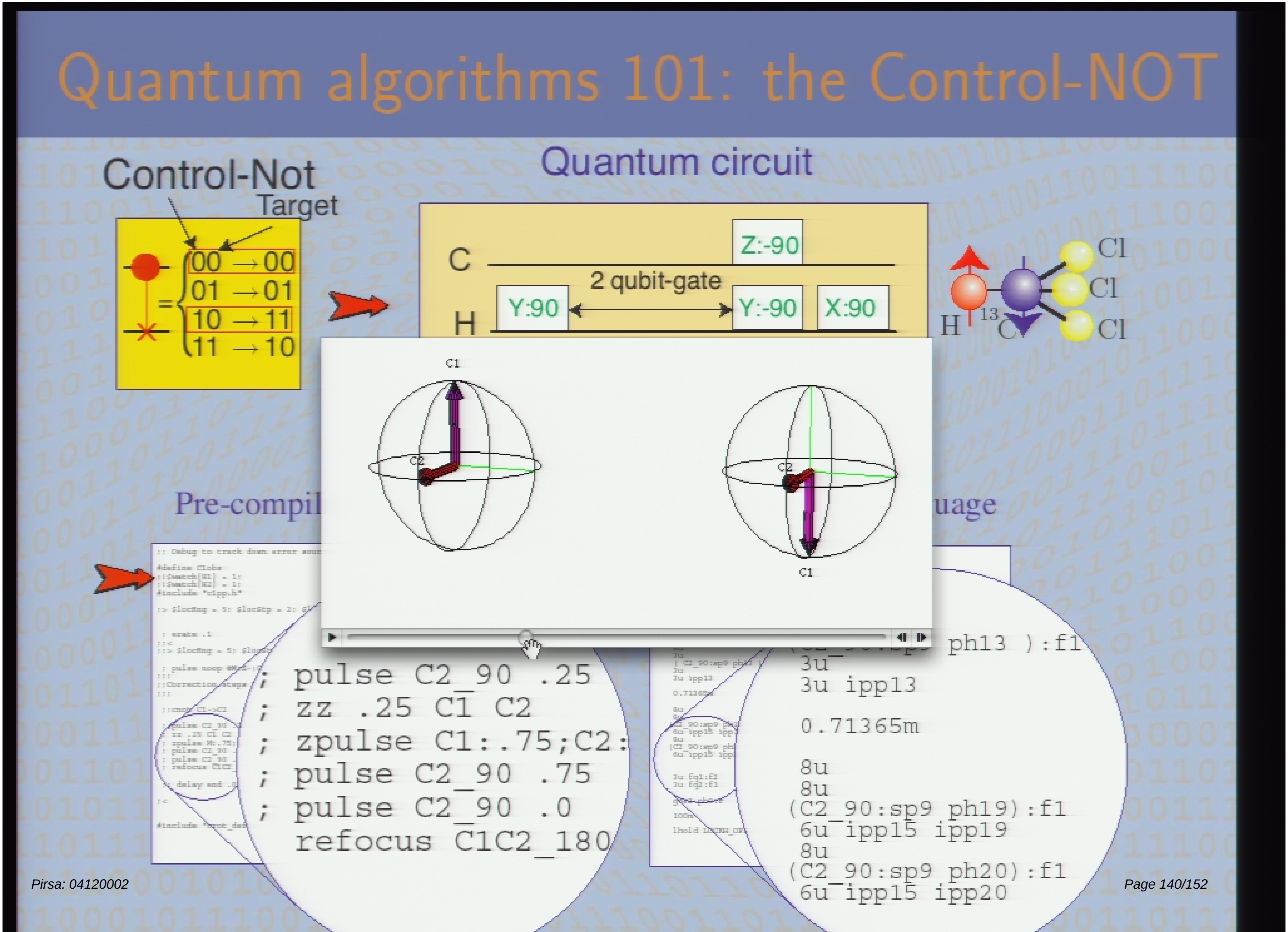
Pre-compil... ...uage

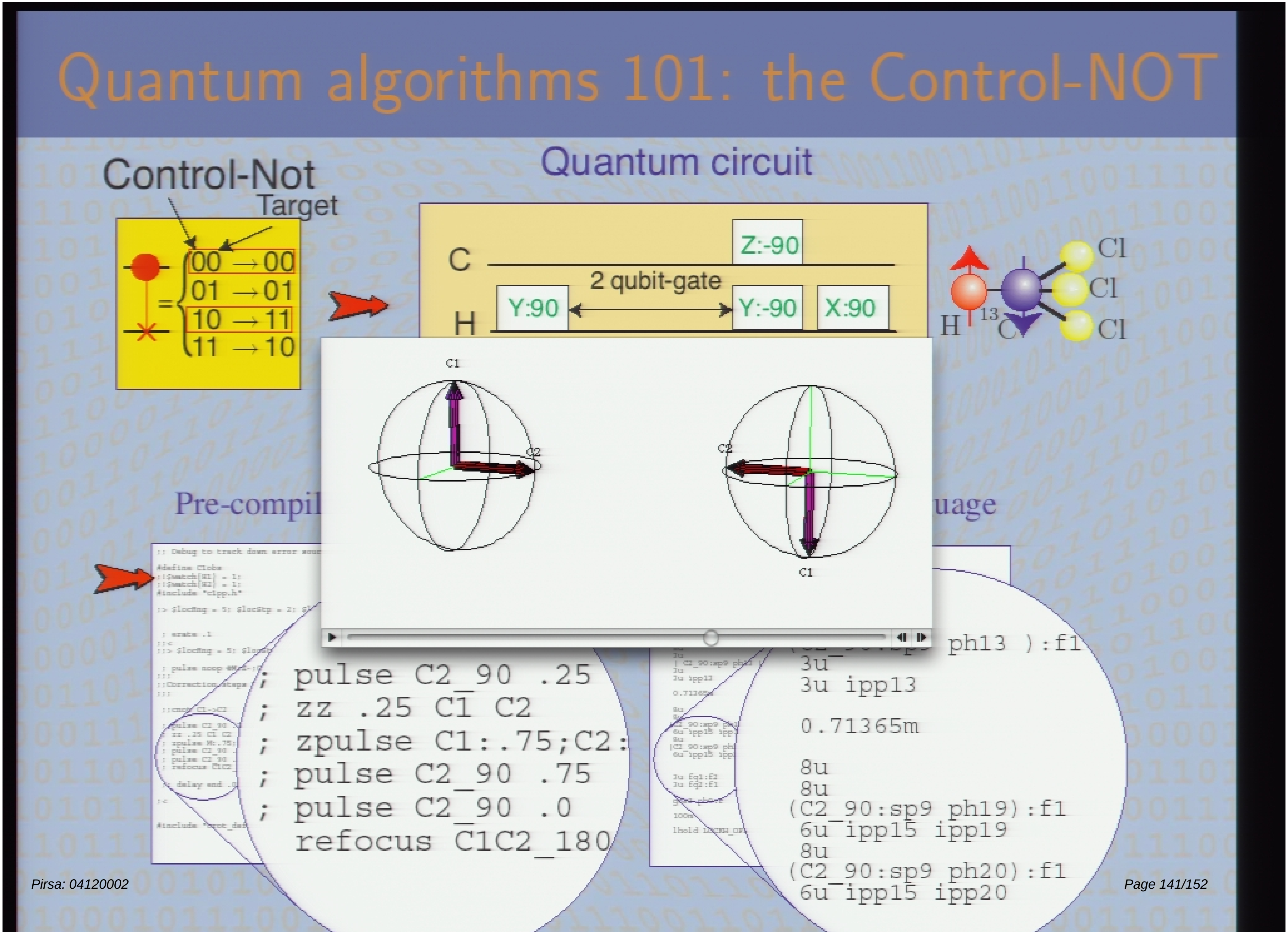
```
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
  refocus C1C2_180
```

```
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
```

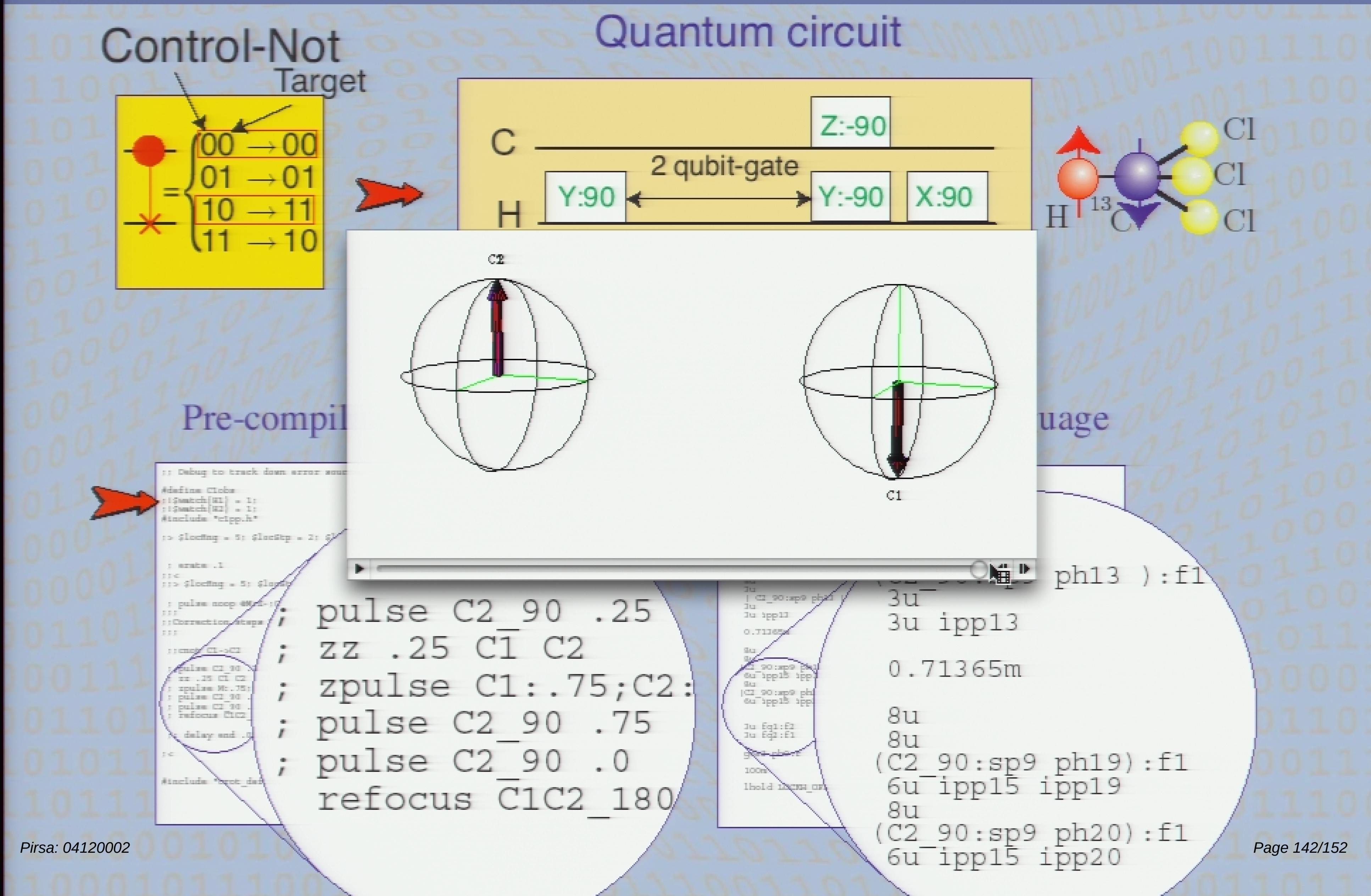

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
Cl
Cl
Cl
H
13
C
C2
C1
Pre-compil
uage
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
ph13):f1
3u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

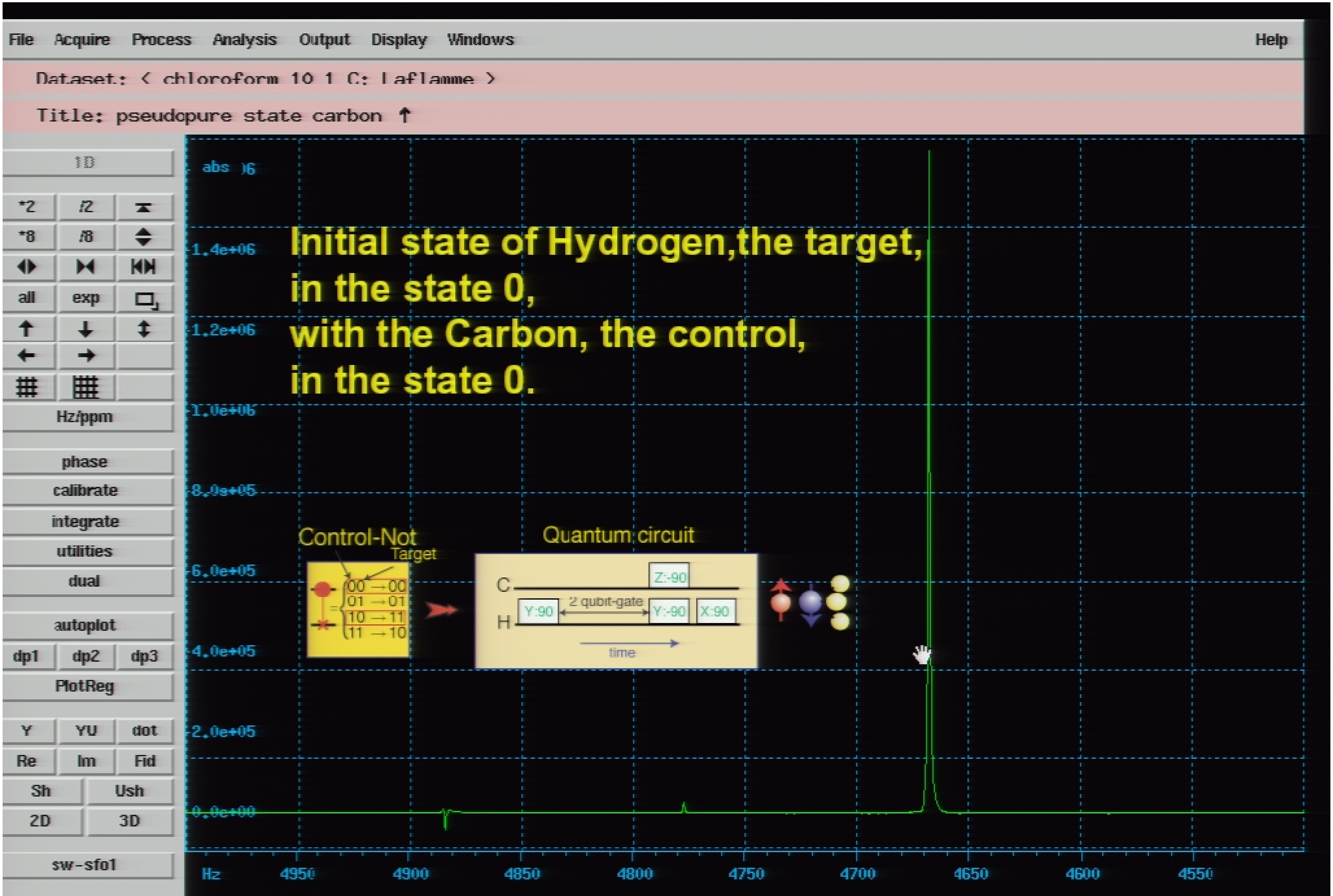

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
Cl
Cl
Cl
H
13
C
C2
C2
C1
Pre-compil
uage
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
ph13):f1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

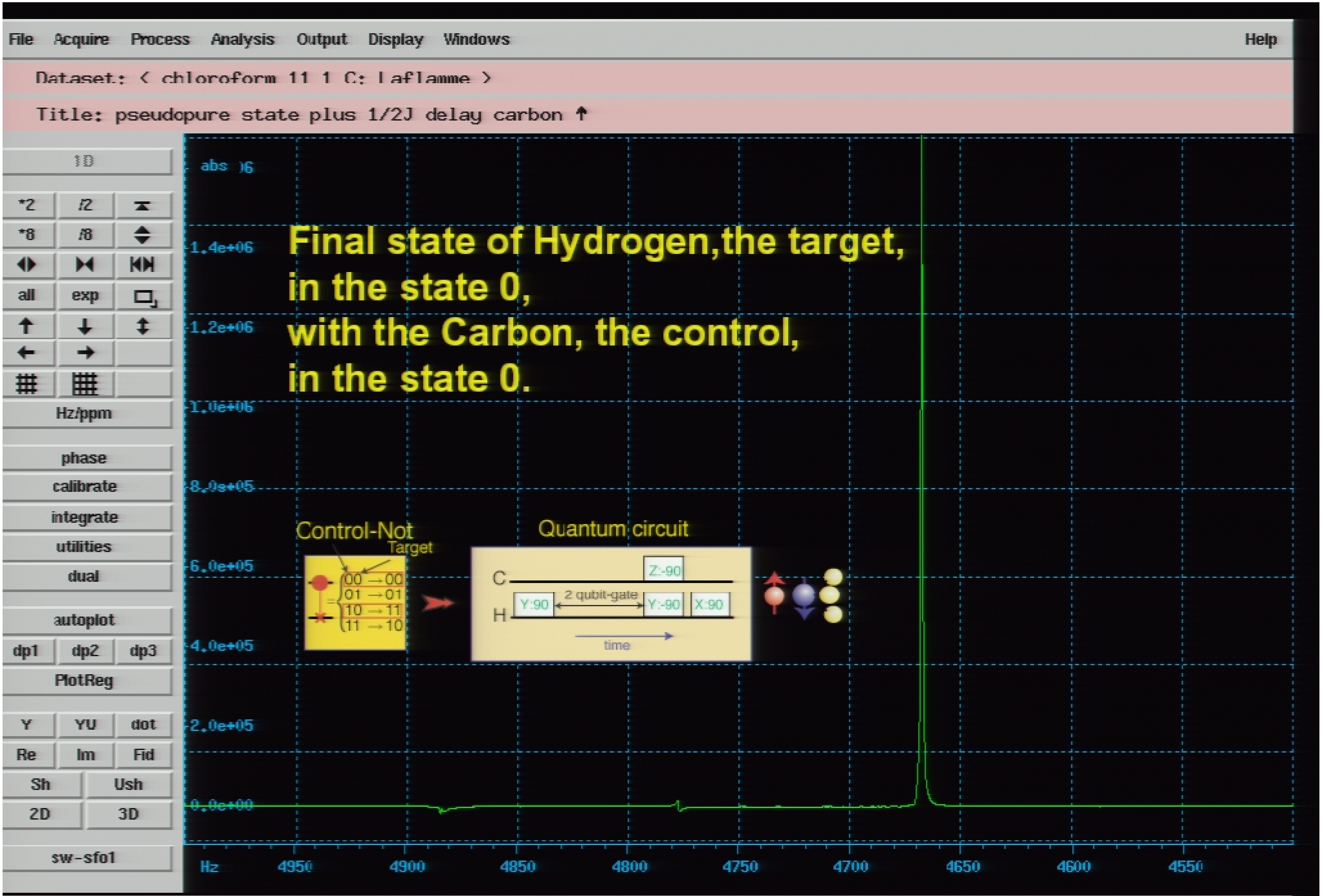

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
Cl
Cl
Cl
H
13
C
C1
C2
Pre-compil
uage
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
ph13):f1
3u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

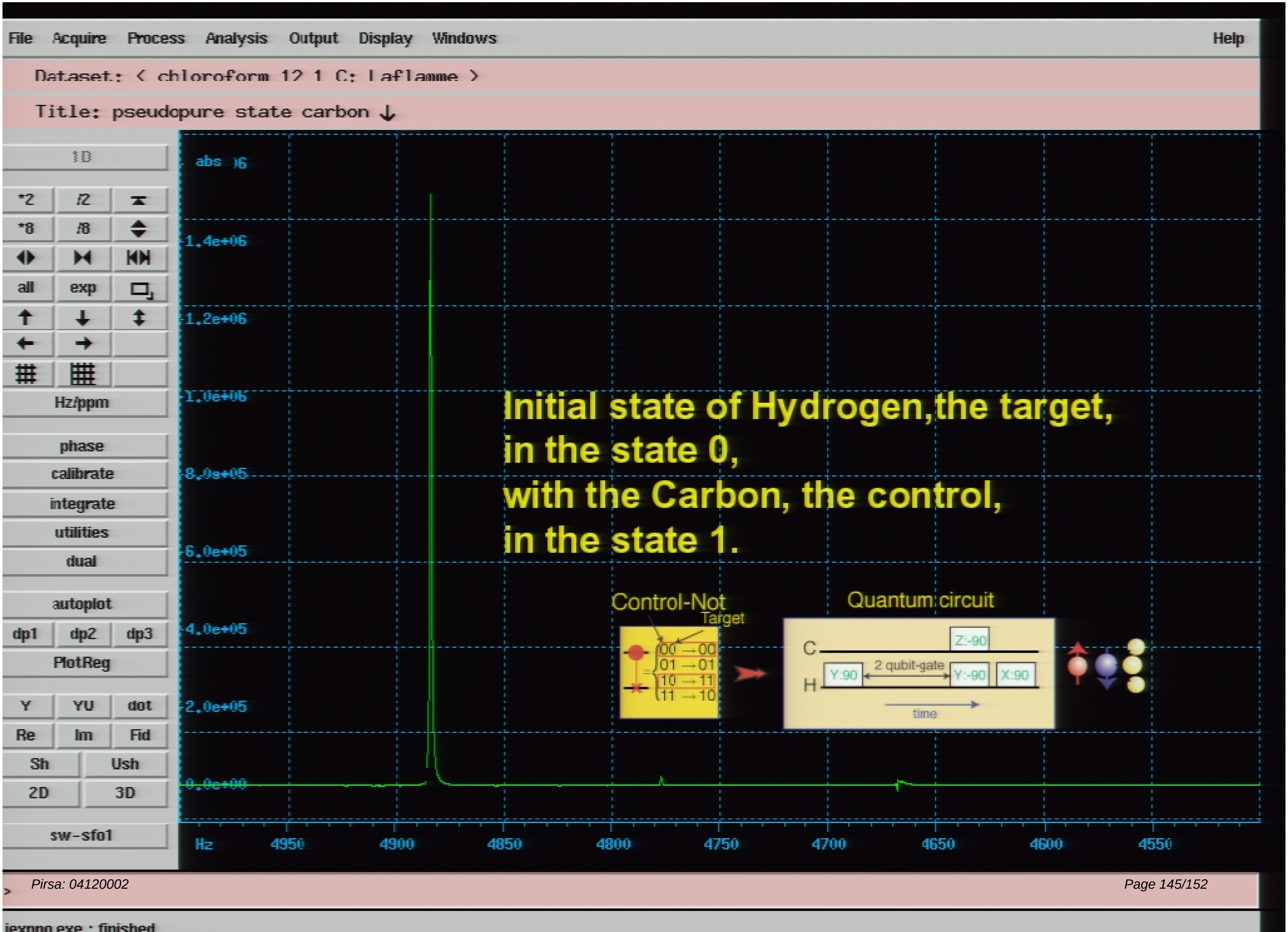

Quantum algorithms 101: the Control-NOT
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
2 qubit-gate
Y:90
Y:-90
X:90
H
13
C
Cl
Cl
Cl
C1
C2
C2
C1
Pre-compil
uage
; pulse C2_90 .25
; zz .25 C1 C2
; zpulse C1:.75;C2:
; pulse C2_90 .75
; pulse C2_90 .0
refocus C1C2_180
ph13):f1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

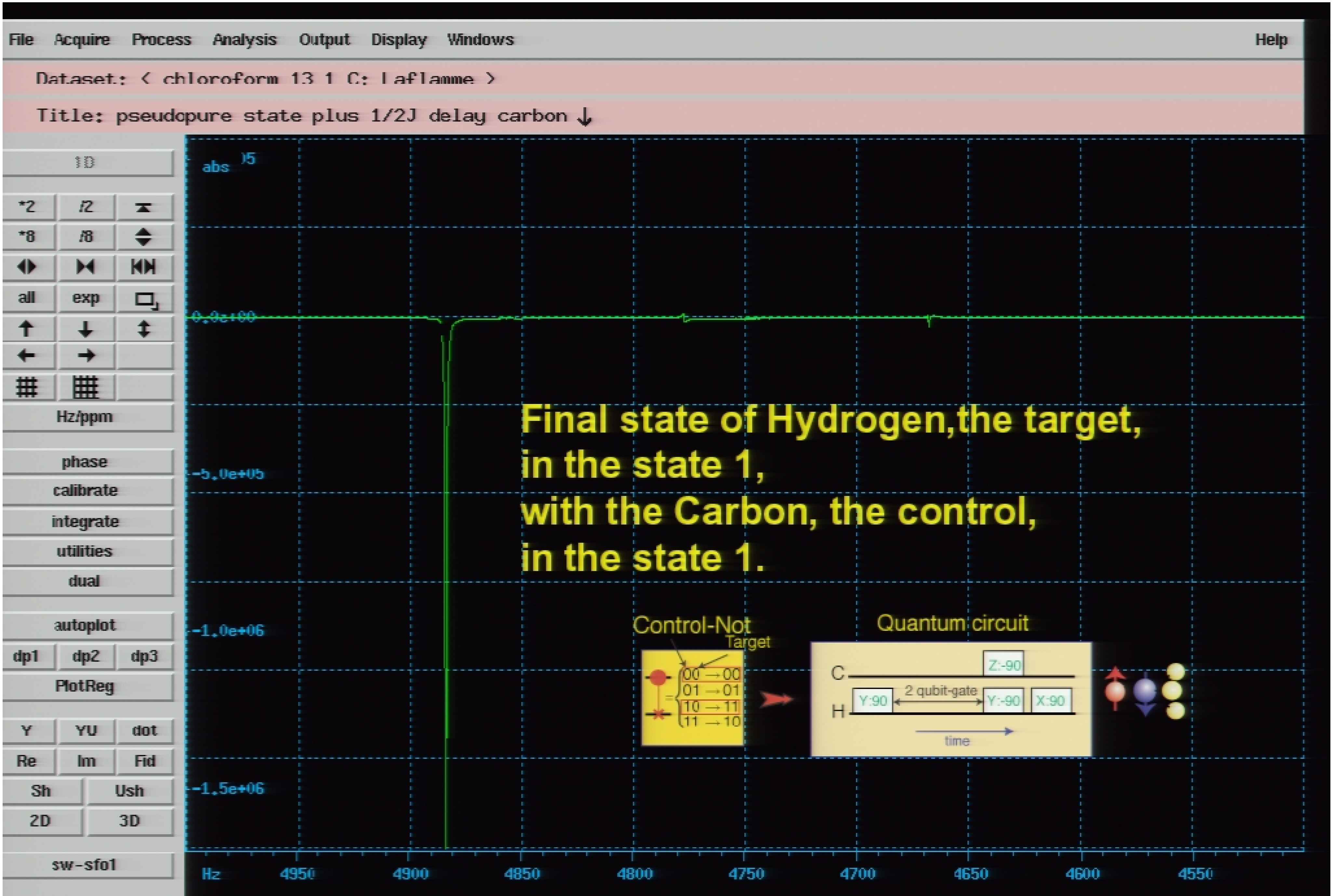
Quantum algorithms 101: the Control-NOT

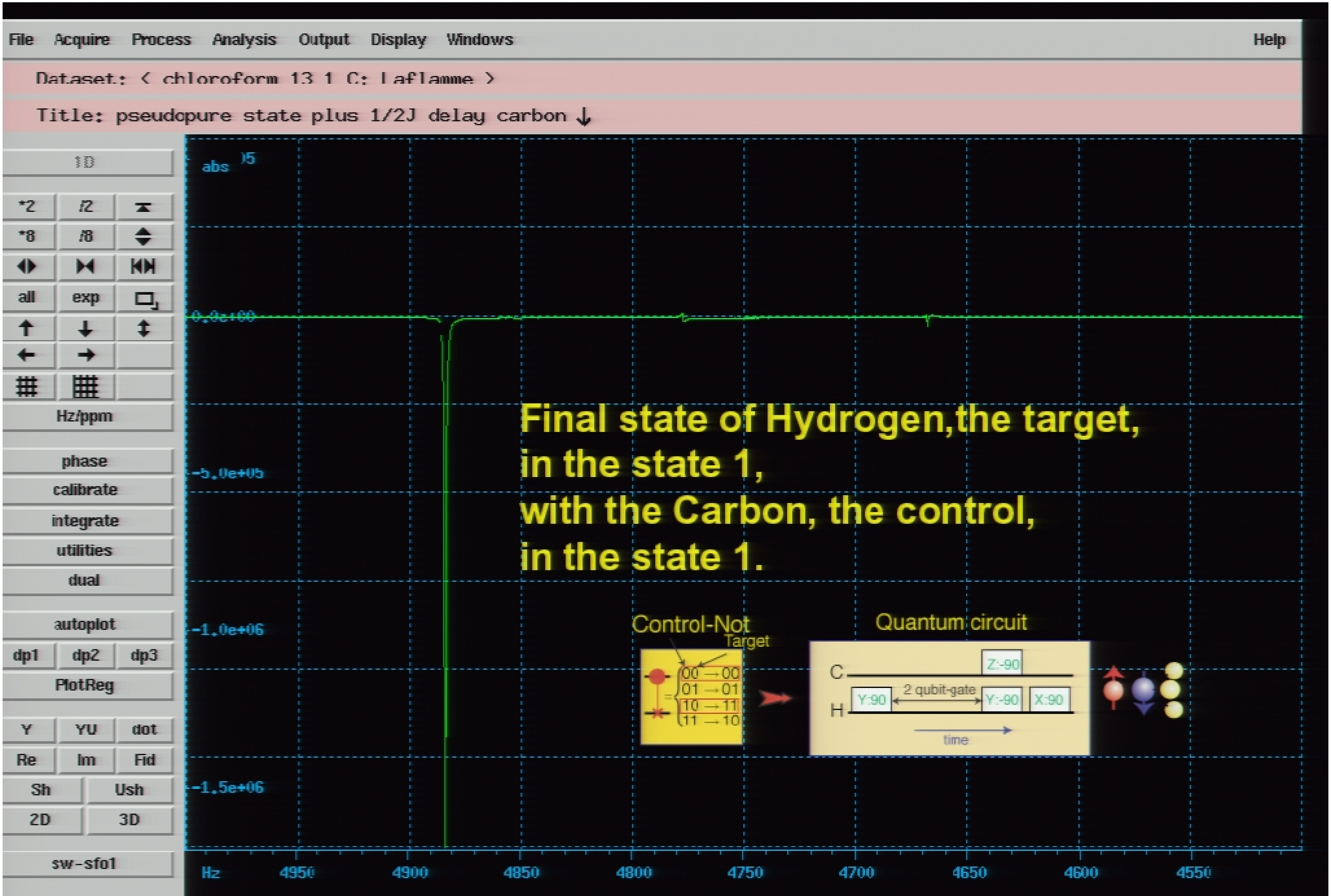



File Acquire Process Analysis Output Display Windows Help
Dataset: < chloroform 10 1 C: laflamme >
Title: pseudopure state carbon
Initial state of Hydrogen,the target,
in the state 0,
with the Carbon, the control,
in the state 0.
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
Y:90
2 qubit-gate
Y:-90
X:90
time
abs
1.4e+06
1.2e+06
1.0e+06
8.0e+05
6.0e+05
4.0e+05
2.0e+05
0.0e+00
Hz 4950 4900 4850 4800 4750 4700 4650 4600 4550
1D
*2 /2
*8 /8
all exp
Hz/ppm
phase
calibrate
integrate
utilities
dual
autoplot
dp1 dp2 dp3
PlotReg
Y YU dot
Re Im Fid
Sh Ush
2D 3D
sw-sfo1

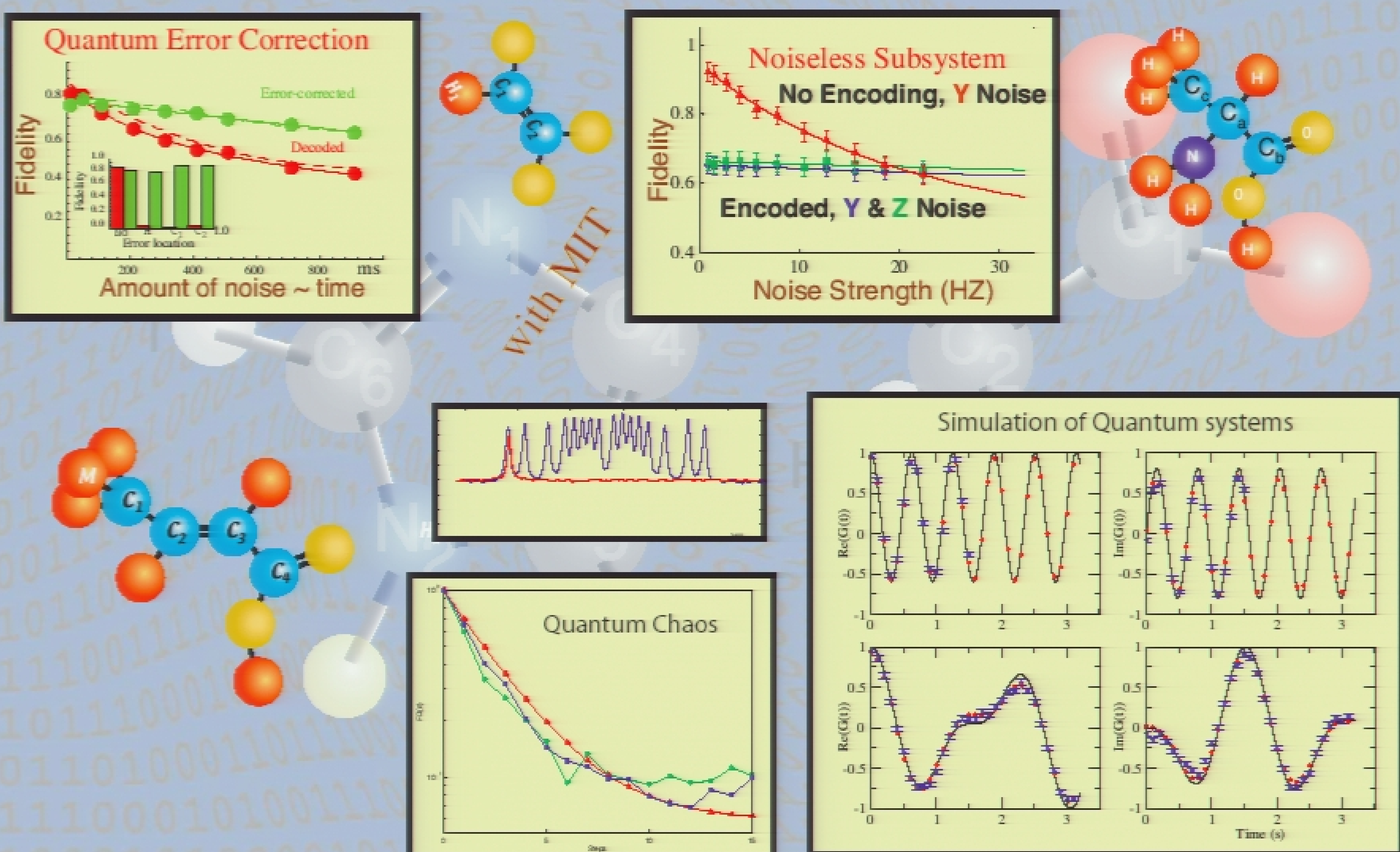

File Acquire Process Analysis Output Display Windows Help
Dataset: < chloroform 11 1 C: laflamme >
Title: pseudopure state plus 1/2J delay carbon
Final state of Hydrogen,the target,
in the state 0,
with the Carbon, the control,
in the state 0.
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
Y:90
2 qubit-gate
Y:-90
X:90
time
1.4e+06
1.2e+06
1.0e+06
8.0e+05
6.0e+05
4.0e+05
2.0e+05
0.0e+00
Hz 4950 4900 4850 4800 4750 4700 4650 4600 4550
phase
calibrate
integrate
utilities
dual
autoplot
dp1 dp2 dp3
PlotReg
Y YU dot
Re Im Fid
Sh Ush
2D 3D
sw-sfo1


File Acquire Process Analysis Output Display Windows Help
Dataset: < chloroform 12 1 C: Laflamme >
Title: pseudopure state carbon
1D
all exp
Hz/ppm
phase
calibrate
integrate
utilities
dual
autoplot
dp1 dp2 dp3
PlotReg
Y YU dot
Re Im Fid
Sh Ush
2D 3D
sw-sfo1
abs
1.4e+06
1.2e+06
1.0e+06
8.0e+05
6.0e+05
4.0e+05
2.0e+05
0.0e+00
Hz 4950 4900 4850 4800 4750 4700 4650 4600 4550
Initial state of Hydrogen, the target, in the state 0, with the Carbon, the control, in the state 1.
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
Y:90
2 qubit-gate
Y:-90
X:90
time
iexpnmr.exe : finished

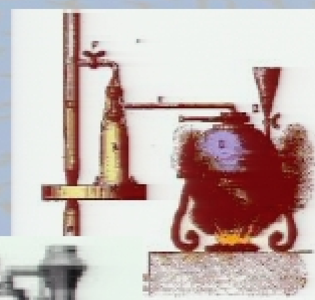

File Acquire Process Analysis Output Display Windows Help
Dataset: < chloroform 13 1 C: laflamme >
Title: pseudopure state plus 1/2J delay carbon ↓
1D
*2 /2
*8 /8
all exp
Hz/ppm
phase
calibrate
integrate
utilities
dual
autoplot
dp1 dp2 dp3
PlotReg
Y YU dot
Re Im Fid
Sh Ush
2D 3D
sw-sfo1
abs
-5.0e+05
-1.0e+06
-1.5e+06
Hz 4950 4900 4850 4800 4750 4700 4650 4600 4550
Final state of Hydrogen,the target,
in the state 1,
with the Carbon, the control,
in the state 1.
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
Y:90
2 qubit-gate
Y:-90
X:90
time


File Acquire Process Analysis Output Display Windows Help
Dataset: < chloroform 13 1 C: laflamme >
Title: pseudopure state plus 1/2J delay carbon
Final state of Hydrogen,the target,
in the state 1,
with the Carbon, the control,
in the state 1.
Control-Not
Target
00 → 00
01 → 01
10 → 11
11 → 10
Quantum circuit
C
H
Z:-90
Y:90
2 qubit-gate
Y:-90
X:90
time
Hz
4950
4900
4850
4800
4750
4700
4650
4600
4550
-5.0e+05
-1.0e+06
-1.5e+06
phase
calibrate
integrate
utilities
dual
autoplot
PlotReg
Hz/ppm
sw-sfo1

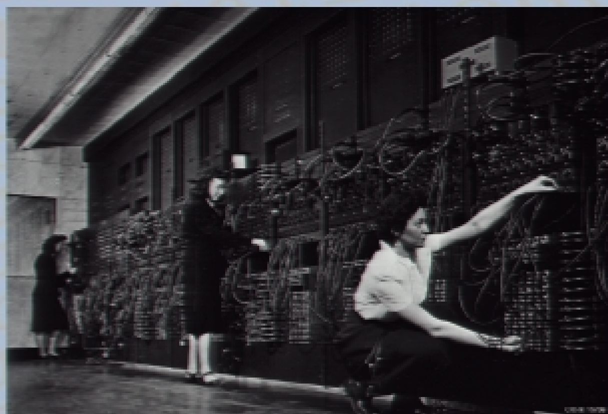
Expt. on small QIP:



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.
- The Institute for Quantum Computing at the University of Waterloo and Perimeter Institute are poised to take advantage of this incredible opportunity.

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

Thanks to:

Institute *for* Quantum Computing