
CS290A, Spring 2005:

**Quantum Information &
Quantum Computation**

Wim van Dam

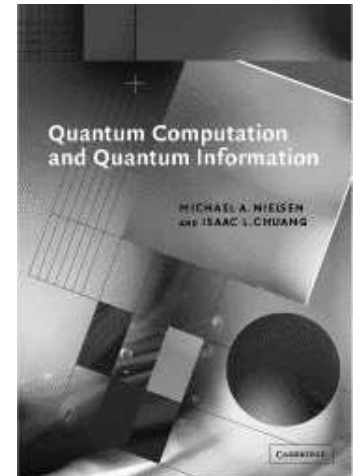
Engineering 1, Room 5109

vandam@cs

<http://www.cs.ucsb.edu/~vandam/teaching/CS290/>

Administrivia

- Required book: M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press. Both editions are fine.
- Home work **suggestions** will be made on Friday.
- Midterm examination in the week of April 25.
- Final project will be determined after the Midterm.
- *Panta rei*: Always check the course web site for the latest information: ~vandam/teaching/CS290/
- Questions?



Mathematics of the Course

- Aimed at graduate students in theoretical computer science.
- Prerequisites: Know your math, especially linear algebra.

“A quantum bit is represented by a two dim. vector with complex valued coefficients $(\alpha, \beta) \in \mathbb{C}^2$. The probability of observing the value “0” when measuring the qubit is calculated by $|\alpha|^2$, while the probability for “1” is $|\beta|^2$. As these probabilities have to sum up to one, we see that $|\alpha|^2 + |\beta|^2 = 1$ (the normalization condition), hence the valid description of a quantum bit corresponds to a vector in \mathbb{C}^2 with length (L_2 -norm) one, and vice versa.”

For the Physicists Among You

From an earlier email:

I do not assume any specific CS knowledge beyond the obvious: an appreciation of the facts that a computation can be decomposed into a circuit of elementary Boolean operation, that the minimal number of such operations indicates the computational complexity of a problem, and that computational complexity is interesting.

For the Most of You

- I do not assume any specific knowledge about quantum mechanics, or physics in general.
- I do rely on the assumption that everyone here has an interest in physics: Studying quantum computing without wanting to learn what quantum physics is about is almost impossible.

Should I Stay or Should I Go?

Stay

- People that are interested in non-standard computers.
- Computer Scientists that are interested in what physics has to say about computational complexity.
- Physicists that are interested in what computer science has to say about quantum physics.

Go

- People that are interested in physical implementations of quantum computers.
- — the philosophy of quantum mechanics
- — “Quantum Programming Languages”

This Week

Raison d'être of quantum computing:

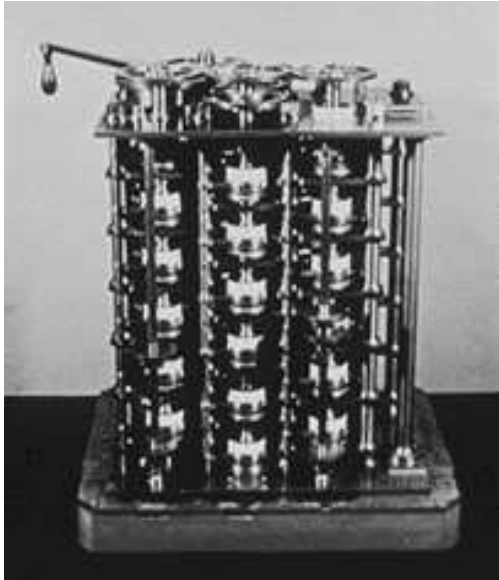
- Events leading up to the formulation of the idea of a quantum information and quantum computing.
- “For better or for worse?” What to like or dislike about quantum computers?

The Language of Quantum Physics:

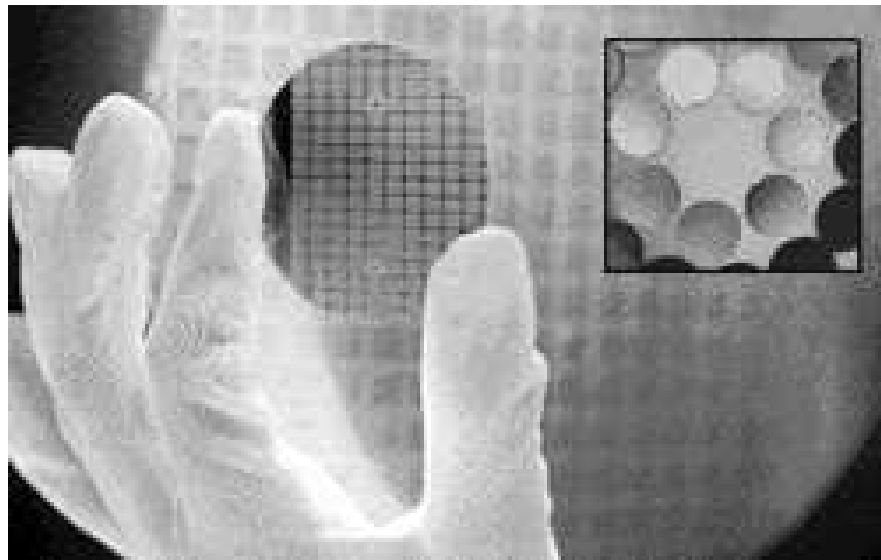
- A sliver of quantum mechanics: the two slit experiment, superpositions, amplitudes, probabilities and nonlocal effects in Nature.

Moore's Law says: The Future is Quantum

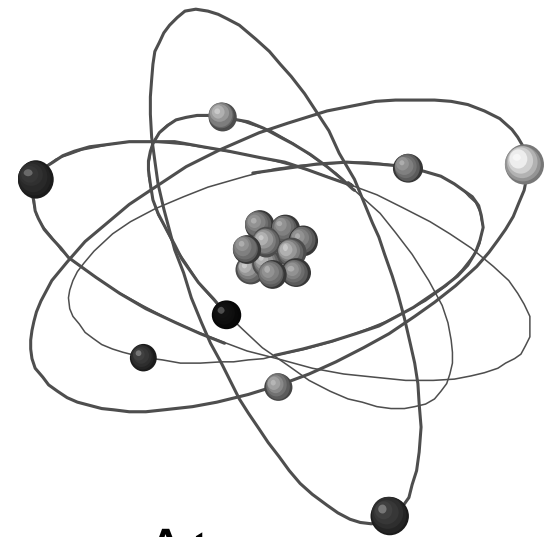
Every 18 months microprocessors double in speed
FASTER = SMALLER



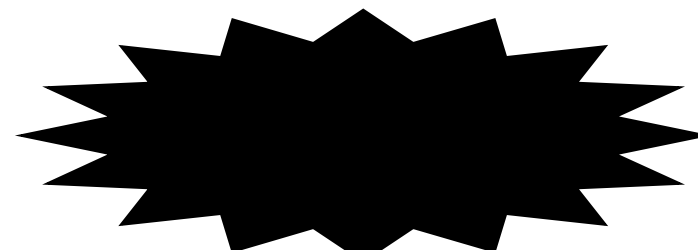
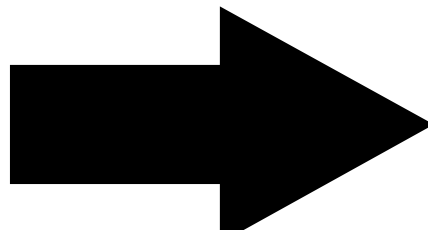
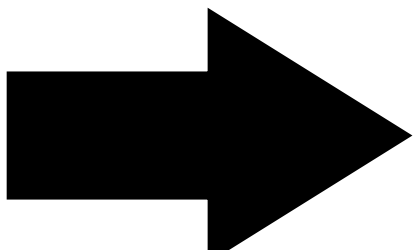
Babbage's
Engine



Silicon Wafers

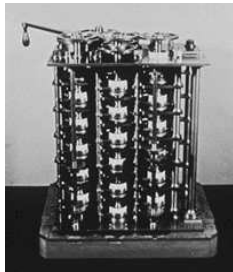


Atoms

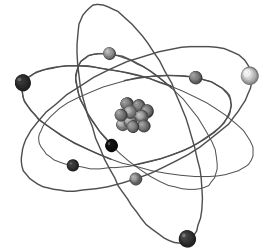
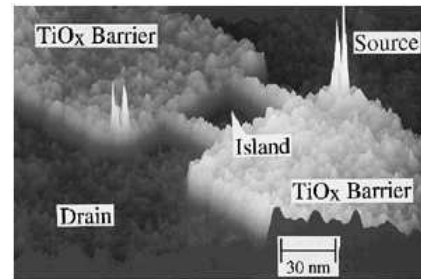
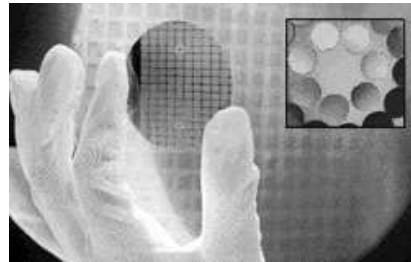


For Better or for Worse?

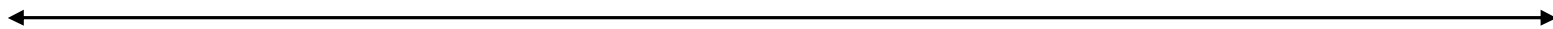
Faster \Rightarrow smaller \Rightarrow shrinking computer



1m



1nm

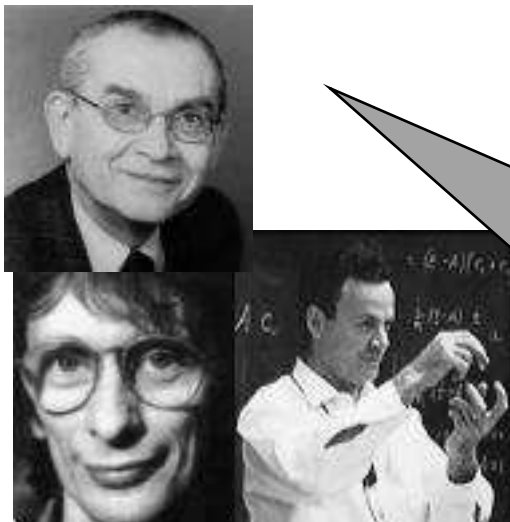


But, at the atomic scale Nature does not work the way we are used to in our macroscopic lives...

At first glance it seems that quantum mechanics (with its uncertainty principle, probabilistic nature) is something to avoid when building a reliable computer.

I love the 80's

- Yu. Manin [1980]: “Computable and uncomputable”, *Sovetskoye Radio*, Moscow (in Russian).
- Richard Feynman [1982]: “Simulating Physics with computers”, *International Journal of Theoretical Physics*, Vol. 21, No. 6,7 pp. 476–488.
- David Deutsch [1985]: “Quantum theory, the Church-Turing principle and the universal quantum computer”, *Proc. Royal Society of London A*, Vol. 400, pp. 97–117.



Quantum physics appears hard to simulate on a traditional computer...a computer with quantum mechanical components could be more powerful than a traditional one.

Quantum Computing

The theory of quantum physics tells us how to calculate the behavior of a quantum mechanical system. As we will see, these calculations will become very lengthy, even for small systems.

The fact that 'Nature' (apparently) has no problems performing these computations lies at the heart of the potential power of a quantum mechanical computing device.

Breaking Cryptography

...In 1994, Peter Shor showed that a **quantum** computer can factorize an n-bit number in $O(n^3)$ time steps. A fully functioning quantum computer implies the end of RSA security and other cryptographic protocols.

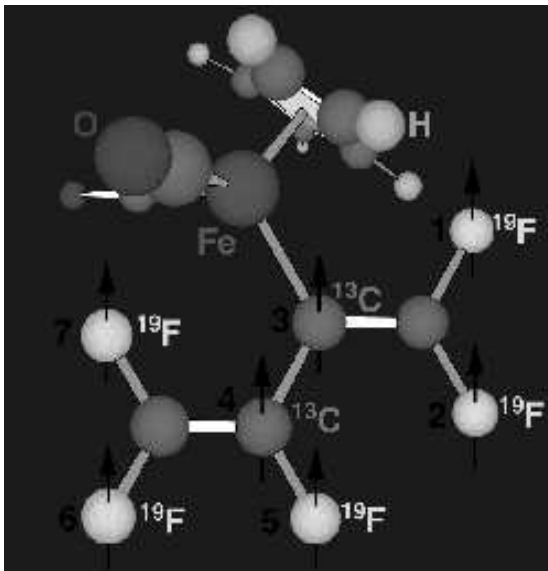


*If the computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get crypto that's quantum, and daunt 'em.*

Experimental, State-of-the-Art Quantum Computing

Making a reliable quantum computer is very difficult:
They are very susceptible to noise and errors.

But the pay-off would be significant: breaking
cryptographic messages (of the past) is worth a lot to
a lot of people (1 billion US\$ and counting).



Currently, the best that has
been done is factoring 15:
(IBM 2001)

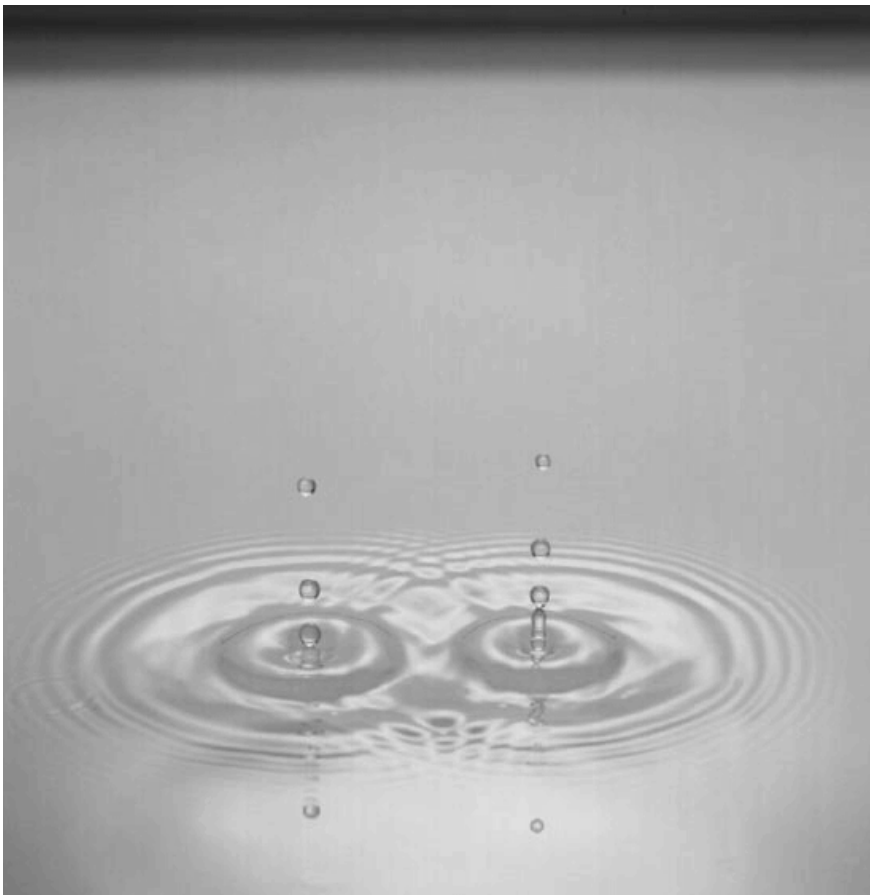


Quantum Mechanics

Quantum mechanics has been battle tested for more than a century now. It is the most accurate theory of Nature that we have.

A quantum mechanical system can be in a **superposition** (parallel, linear combination) of basis states.

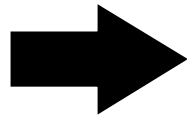
Unlike classical probabilities, these states can **interfere** (interact) with each other.



Superposition of States

Classical Bit

0 or 1

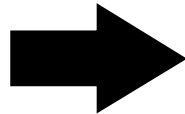


Quantum Bit

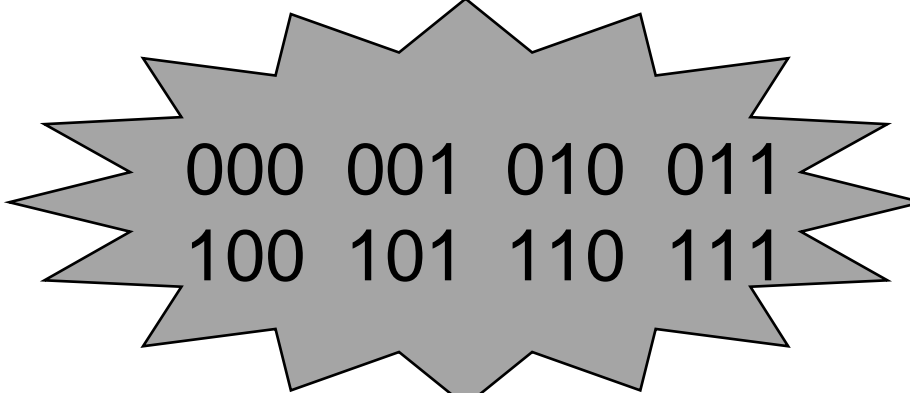
0 or 1 or 

Classical register

101

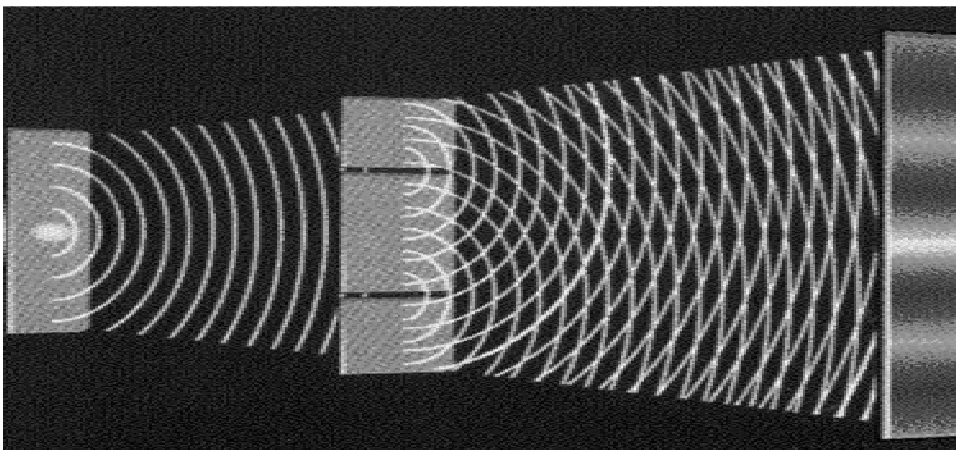


Quantum register

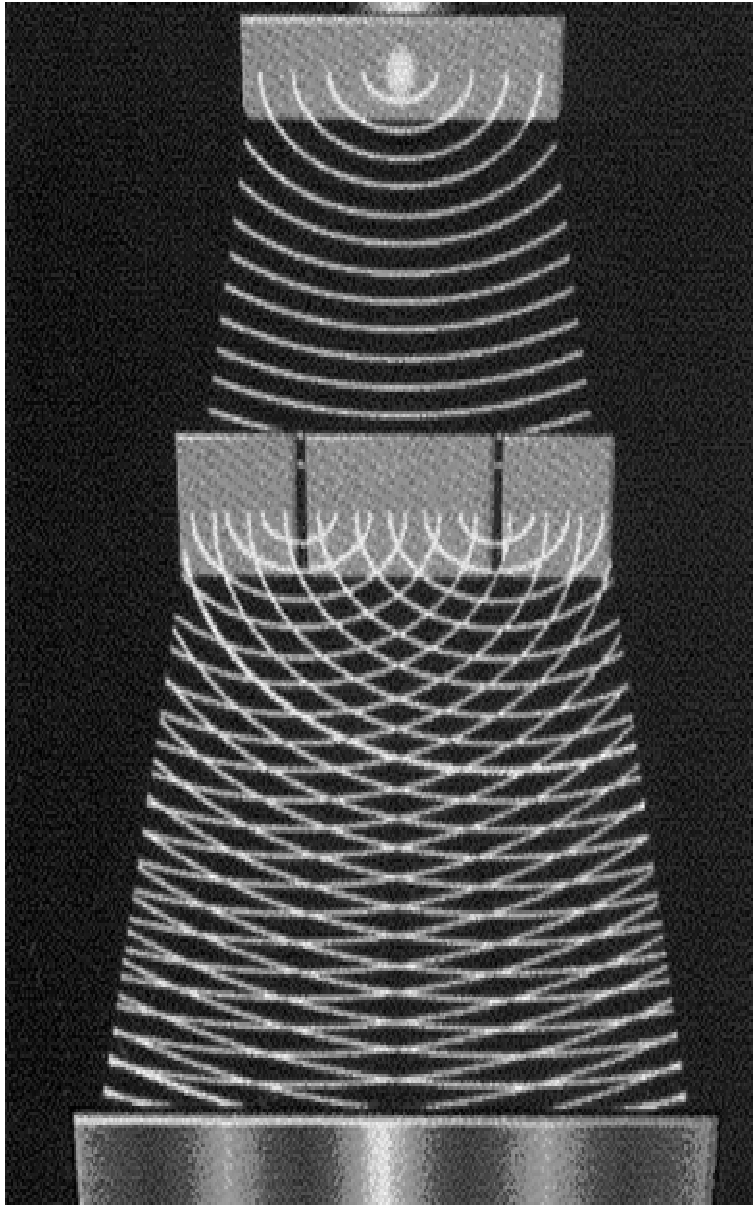


000 001 010 011
100 101 110 111

Just like the photons in
a two-slit interference
experiment.



The Two Slit Experiment



Consider the trajectory of a single photon in the double slit experiment.

The only way we can explain interference at extremely low intensities is by assuming that the particle goes through both slits at the same time: it is in a **superposition** of going through the left slit and the right slit.

Afterwards, these two possibilities can **interfere**.

Bullets versus Waves

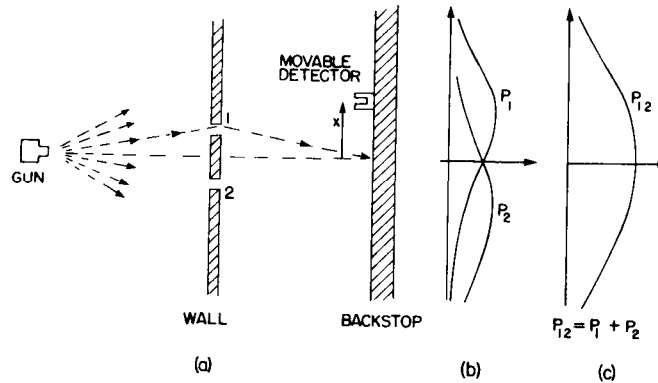


Fig. 1-1. Interference experiment with bullets.

Bullets: Add the probabilities to get final outcome.

Water waves:
Final outcome
is determined not
only by heights;
also by phases of
incoming waves.

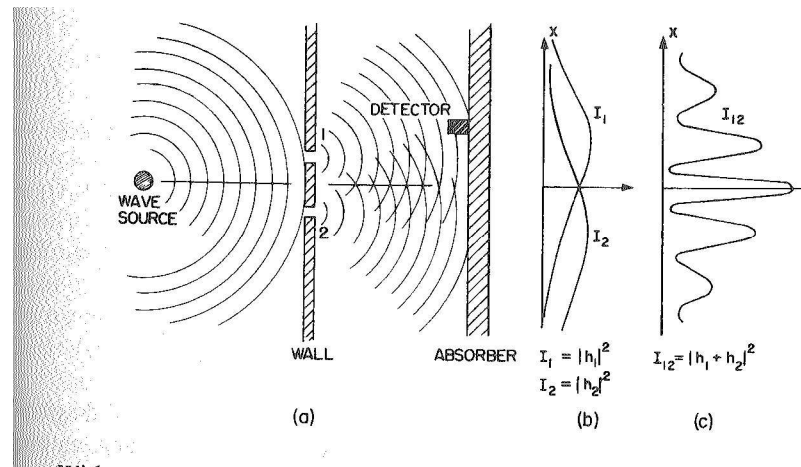
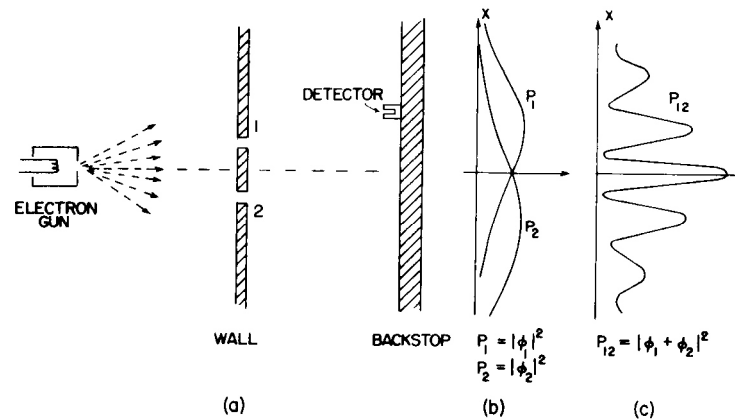


Fig. 1-2. Interference experiment with water waves.

Particles as Waves

Fig. 1-3. Interference experiment with electrons.



1-4

Electrons:
Final outcome is best described if we assume that electrons behave like waves.

Experiments show: To describe the behavior of particles like photons, electrons, et cetera, you should replace classical event probabilities $p_1, p_2, \dots \in [0, 1]$ by complex valued *amplitudes* $\alpha_1, \alpha_2, \dots \in \mathbb{C}$. “Amplitudes squared”, $|\alpha_1|^2$, give probabilities.

Quantum Mechanics

A system with D basis states is in a superposition of all these states, which we can label by $\{1, \dots, D\}$.

Associated with each state is a complex valued amplitude; the overall state is a vector $(\alpha_1, \dots, \alpha_D) \in \mathbb{C}^D$.

The probability of observing state j is $|\alpha_j|^2$.

When combining states/events you have to add or multiply the amplitudes involved.

Examples of Interference:

Constructive: $\alpha_1 = 1/2$, $\alpha_2 = 1/2$, such that $|\alpha_1 + \alpha_2|^2 = 1$

Destructive: $\alpha_1 = 1/2$, $\alpha_2 = -1/2$, such that $|\alpha_1 + \alpha_2|^2 = 0$

(Probabilities are similar but with \mathbb{R} instead of \mathbb{C} .)

Terminology

complex amplitude $\alpha \in \mathbb{C}$

magnitude $r \in [0, 1]$

$$\alpha = a + bi = re^{i\varphi} \quad \leftarrow \text{phase } \varphi \in [0, 2\pi)$$

real part $a \in [-1, 1]$

imaginary part $b \in [-1, 1]$

“Amplitudes squared”:

$$|\alpha|^2 = a^2 + b^2 = r^2$$

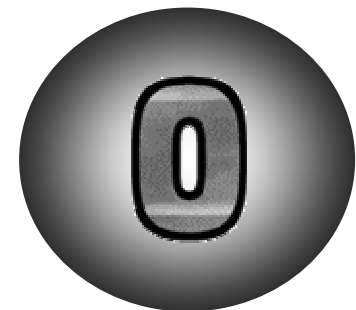
Complex conjugates:

$$\alpha^* = \bar{\alpha} = a - bi = re^{-i\varphi}$$

Note $|\alpha|^2 = \alpha\alpha^*$.

Quantum Bits (Qubits)

- A single quantum bit is a linear combination of a two level quantum system: {"zero", "one"}.
- Hence we represent that state of a qubit by a two dimensional vector $(\alpha, \beta) \in \mathbb{C}^2$.
- When observing the qubit, we see "0" with probability $|\alpha|^2$, and "1" with probability $|\beta|^2$.
- Normalization: $|\alpha|^2 + |\beta|^2 = 1$.
- Examples: "zero" = $(1, 0)$, "one" = $(0, 1)$,
uniform superposition = $(1/\sqrt{2}, 1/\sqrt{2})$
another superposition = $(1/\sqrt{2}, i/\sqrt{2})$



Quantum Registers

- Generalizing, a string of n qubits has 2^n different **basis states** $\{0,1\}^n$. The quantum state has thus $N=2^n$ complex amplitudes $(\alpha_1, \dots, \alpha_N) \in \mathbb{C}^N$.
- The probability of observing $x \in \{0,1\}^n$ is $|\alpha_x|^2$.
- The amplitudes have to obey the normalization restriction:
$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$
- The $x \in \{0,1\}^n$ -vectors are the **classical basis states**.
- Examples for $n=3$ quantum bits:
"000" = $(1, 0, 0, 0, 0, 0, 0, 0)$
... = $(\alpha_{000}, \alpha_{001}, \alpha_{010}, \alpha_{011}, \alpha_{100}, \alpha_{101}, \alpha_{110}, \alpha_{111})$

Dirac's Ket Notation



- To use notation like $(\alpha_{000}, \dots, \alpha_{111})$ gets very tedious.
- Instead we will use the bracket notation of Paul Dirac where if we have the basis state $s \in S$, then the corresponding basis vector is denoted by $|s\rangle$. Instead of v_s or $(0, \dots, 0, 1_s, 0, \dots, 0)$.
- Think of $|s\rangle$ as a basis vector in column orientation.
- General superpositions are also expressed as kets.
- Advantage: we can put anything as label text.
- The following is perfectly okay mathematically:

$$|\text{uniform superposition of qubit}\rangle = \frac{1}{\sqrt{2}}|\"0\"\rangle + \frac{1}{\sqrt{2}}|\"1\"\rangle$$

Ease of Ket Notation

- The state ψ of n qubits with its 2^n amplitudes can be described as the (linear) summation:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$$

- The $x \in \{0,1\}^n$ -vectors are again the classical basis states.
- From now on, we will use use the ket-notation.
- “They’re just vectors!”, Lance Fortnow

Measuring is Disturbing

- If we measure the quantum state $|\psi\rangle$ in the computational basis $\{0,1\}^n$, then we will measure the outcome $s \in \{0,1\}^n$ with probability $|\alpha_s|^2$.
- For the rest, this outcome is fundamentally random. (Quantum physics predicts probabilities, not events.)
- Afterwards, the state has ‘collapsed’ according to the observed outcome: $|\psi\rangle \mapsto |s\rangle$, which is irreversible: all the prior amplitude values α_x are lost.