Phys 396 2026

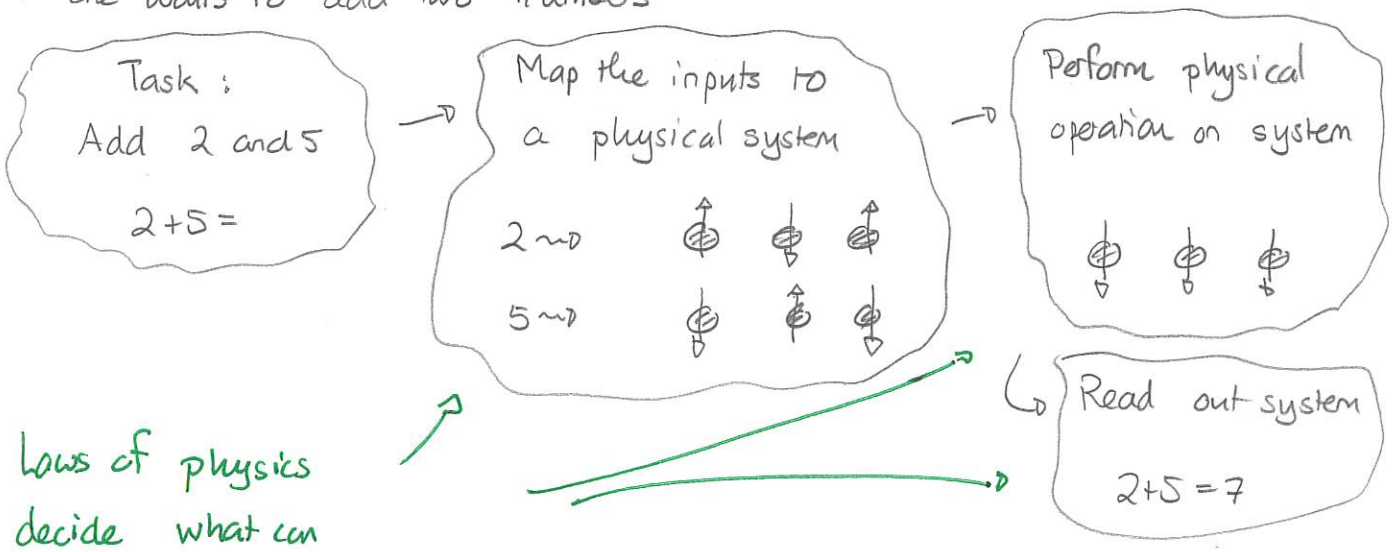
Lecture 1

* Syllabus
* Course Website.
* Assignments - typically due Fridays
  - first Fri, Aug 21
* Exams - three in class - check dates on syllabus
* Class project + presentation last part of semester.
* Weds 1.2.1.

Quantum Information

Quantum information considers how to use physical systems that obey the laws of quantum theory to do information processing tasks. It also considers how to use the framework of information theory to describe aspects of quantum systems. This course will focus on how to use quantum physics to do information processing.

In this context quantum information takes the viewpoint that one must consider the physical resources required to do any information processing task. For example, if one wants to add two numbers



Quantum information says that the relevant laws of physics that determine how one can do the information processing are the laws of quantum physics. It turns out that harnessing some of the strange aspects of quantum physics allows us to (potentially)

* factorize a large number efficiently
* search an unsorted database with fewer steps that require by any device restricted to classical physics
* simulate physical systems more effeciently than can be done with a device restricted to classical physics
* share cryptographic keys with a security that cannot be attained otherwise
* improve the resolution of measuring + sensing devices.

Note that the approach to these will be physics-based. It is necessary to know and use the underlying physics to devise, use and evaluate quantum information processing schemes. This has two broad pieces.

1) Theory * use the laws of quantum physics to provide schemes for information processing

Demo: - Show aspects of my paper with Jaime
- Show Grover algorithm circuit

2) Experiment / realization * theoretical procedures must be converted to practical experimental schemes

Demo: - Show Inflection Page + device
- Show IQM → Technology → Tech Stack.
- Show IBM Quantum Experience...

Over the last decade quantum information devices have grown in size by a factor of 20-30. There are now many businesses offering quantum products and hiring to develop these products

DEMO: - show some corporate websites
- show QED-C page.

Phys 396 Course.

The course will introduce you to the fundamental concepts of quantum physics that are needed to work in and understand quantum information. We will cover some general features of quantum information and some important applications.

Fundamental aspects of classical computing

Certain key ideas from classical computing are important for quantum information and we will review:

1) representation of classical computing and basic computing steps
2) complexity of solving problems

We do these in ways which are generic and independent of the details of a device or hardware. We also ignore details of coding provided that it's efficient. We can illustrate this with an example of factorizing numbers,

Example Factorize.

a) 21
b) 247
c) 1517

Describe the procedure for doing this?
Can you quantify how difficult it is to do the factorization task?

Answer: a) $21 = 3 \times 7$

b) Divide by successive primes 2, 3, 5, 7, 11, 13, 17,

$247 = 13 \times 19$ Had to try six primes.

c) Divide by successive primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...

$1517 = 37 \times 41$ Had to try 12 primes.

It appears that as the number becomes larger the task requires more basic steps and thus more basic resources. Can we quantify this more precisely? This question is an example of computational complexity, in essence how the number of resources needed to solve a problem scales as the size of the inputs increases.

One thing that quantum information provides is methods of reducing the complexity of problems

In order to address questions like this for any given type of problem we need to

State problem
e.g. factorise number.

→ Provide a method for answering the problem in all cases.
e.g. state an algorithm
→ divide by successive primes

→ Count the basic number of steps needed as a function of size of input

Represent input in a quantifiable way
e.g. binary representation

→ Represent mathematical operations in terms of basic operations
e.g. binary addition
binary multiplication

Binary representation of numbers

We can represent any number X as a sum of powers of 2.

$$X = X_0 2^0 + X_1 2^1 + X_2 2^2 + \cdots = \sum_{k=0}^{\infty} X_k 2^k$$

where $X_k = 0$ or 1, is called a binary coefficient. We can represent the number as the string of binary coefficients $X_0, X_1, X_2, \ldots$ usually writing it as

$$X = \cdots X_{n-1} \cdots X_1 X_0$$

which is just a list of digits. (not a product). For finite numbers, the digits will be zero after some non-zero X_{n-1}. Thus we can write

$$X = X_{n-1} X_{n-2} \cdots X_1 X_0$$

Each digit is called a <u>bit</u> and the entire collection is called a <u>bit string</u>. The number of digits in this bit string, n, represents the size of the number.

<u>Example</u> The number 9 is

$$9 = 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

$$X_3 = 1 \quad X_2 = 0 \quad X_1 = 0 \quad X_0 = 1$$

$9 \mapsto 1001$

This is a 4-bit number. So

An n-bit number requires a minimum o

Binary addition

We must be able to add two numbers using their binary representation.

Consider three examples:

1) $2+4$

$4 = 100 = 1\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0$

$2 = 010 = 0\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$

add these $(1+0)\cdot 2^2 + (0+1)\cdot 2^1 + (0+0)2^0$

$= 1\cdot 2^2 + 1\cdot 2^1 + 0\cdot 2^0$

So $4+2 \rightsquigarrow 110 \rightsquigarrow 6$.

2) $2+3$

$2 = 10$

$3 = 11$

Adding bitwise $(1+1)\ 1$

?

Adding two 1's gives a 2. Here that would produce $2\cdot 2^2$

$= 1\cdot 2^3 + 0\cdot 2^2$

So adding two "1"s gives $\rightarrow$ 0

↳ a carry of "1"

Thus

$$\begin{array}{r} 10 \\ 11 \\ \hline 101 \end{array} \equiv 5$$