Quantum Computing

1. Building Blocks of a Quantum Computer

C S Vijay and Vishal Gupta

C S Vijay is in the final year of a dual degree program in microelectronics at the Department of Electrical Engineering at IIT Mumbai. His primary interest is in developing algorithms for performance driven optimization of VLSI circuits.

Vishal Gupta was an undergraduate student at the Department of Electrical Engineering, IIT Mumbai. His interests include quantum computing, physics, telephony, and information theory. He is currently involved with a start-up company at IIT Mumbai.

1. Introduction

In the early 1980s Richard Feynman noted that quantum systems cannot be efficiently simulated on a classical computer. Till then the accepted view was that any reasonable model of computation can be efficiently simulated on a classical computer. Hence, this observation led to a lot of rethinking about the basic models of computation and the physics behind the computation. It was suggested that the dynamics of quantum systems could be used to perform computation in a much more efficient way. After this initial excitement, things slowed down for some time till 1994 when Peter Shor announced his polynomial time factorization algorithm[1] which uses quantum dynamics. The study of quantum systems for computation has come into its own since then. In this article we will look at a few concepts which make this framework so powerful.

2. Quantum Physics Basics

Consider an electron (say, in a H atom) with two energy levels (ground state and one excited state). In general, the electron can be in a superposition of both the states. We represent these 2 'basis' states by $|0\rangle$ and $|1\rangle$ where $|\rangle$ is called a 'ket' (this notation, introduced by Dirac, comes from the two parts of a bracket $\langle\rangle$, the 'bra' $\langle|$ and the 'ket' $|\rangle$). The ket is just a convenient representation for a column vector, for we could have chosen the basis for our system as $(1,0)^T$ and $(0,1)^T$

The state space of a quantum system can be modeled by a finite dimensional complex vector space with an inner

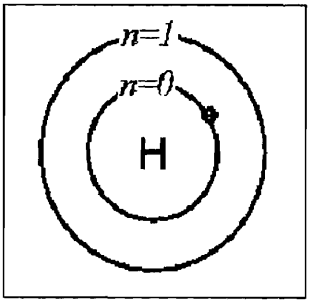


Figure 1. Two energy levels in a H atom.

product. For the above system such a vector space could be any two dimensional complex vector space. Let us call, just as a matter of convention, the $(1,0)^T$ vector as $|0\rangle$ and the $(0,1)^T$ vector as $|1\rangle$. Any state of the electron can thus be represented as $a|0\rangle + b|1\rangle$.

Let us look at Dirac's notation more closely as we are going to make heavy use of it. The inner product of two vectors $|x\rangle$ and $|y\rangle$ is written as the bra-ket combination $\langle x||y\rangle$. For instance, we have $\langle 0||0\rangle = 1$ and $\langle 0||1\rangle = 0$. The outer product $|x\rangle\langle y|$ of two vectors x and y is a linear transformation operator, which is equivalent to the matrix xy^T As an example:

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(10) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

[1] The best known algorithms for factorization under the classical model of computation grow as some non-polynomial function of the number of digits in the number being factored.

Clearly, this is a transformation that maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $(00)^T$ ($(00)^T$ is what you get when you multiply any vector by the scalar 0).

Outer products are very convenient in expressing any kind of transformation on quantum states as we will see later in our discussion on quantum gates.

Now that we have this notation, we will state a very basic fact about quantum states: *as soon as one makes a measurement* [2] *on an unknown quantum state, it* **collapses** *to one of the eigenstates, each measurement having a specific set of eigenstates.* Intuitively one can see this by going back to the electron we had considered. One could argue that the electron would normally be shuttling between states and at any instant we 'freeze' the system(i.e., at the moment of 'measurement') it must be in one of the two basis states. But the result we have stated says more: it says that once we make a measurement the quantum state continues to be in the state measured. Thus,

$$a|0\rangle + b|1\rangle \longrightarrow \text{measure} \longrightarrow |0\rangle or |1\rangle.$$

[2] Refer to section 7.

3. Qubits

The simplest quantum state $a|0\rangle + b|1\rangle$ is called a qubit, or a quantum bit. The qubit could represent any 2 dimensional quantum vector, such as the direction of polarization of a photon or the state of an electron in an atom with just two energy levels. The qubit is normalized such that $|a|^2 + |b|^2 = 1$, so that $|a|^2$ and $|b|^2$ represent the probabilities that, on 'measurement' the qubit is found to be $|0\rangle$ or $|1\rangle$, respectively. Once measured, the qubit continues to remain in the state measured. One could then ask what the probabilities of measurement, $|a|^2$ and $|b|^2$ mean. One has to understand it statistically in this way: if there is a source producing identical qubits (i.e., qubits whose histories are the same), then, in a large collection of such qubits, the ratio of those measured as $|0\rangle$ to those measured as $|1\rangle$ would be $|a|^2$ to $|b|^2$.

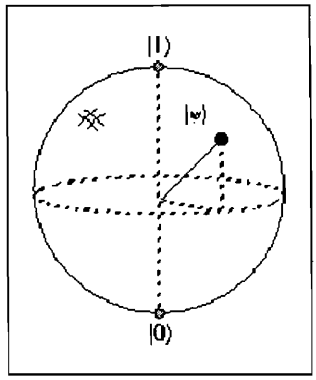


Figure 2. A qubit can take values over the surface of a sphere which has $|0\rangle$ and $|1\rangle$ as its poles.

One might make the mistake of supposing that since a qubit can take values over a disc (or the surface of a sphere), it can contain an infinite amount of information. However, all this information is not available to us, as the result of any measurement can only be one of the 2 eigenstates. Thus, all that information is 'hidden' from us. Quantum algorithms, as we shall see in the second part of this article, are based on extracting some features of this 'hidden information' from a collection of qubits.

4. Multiple Qubit Systems

When quantum systems combine, the resultant state space of the combined system is obtained by the tensor product (henceforth represented by $\otimes$) of the state spaces of the combining systems.

Let us first examine the differences between the tensor product and Cartesian product. Consider two systems with basis states as (p_1, p_2, p_3) and (q_1, q_2). If the sys-

tems combine through the Cartesian product then the basis set of the combined system is given by $(p_1, p_2, p_3, q_1, q_2)$; on the other hand, if the systems combine through the tensor product then the associated basis set for the combined system is given by $(p_1 \otimes q_1, p_1 \otimes q_2, p_2 \otimes q_1, p_2 \otimes q_2, p_3 \otimes q_1, p_3 \otimes q_2)$. Thus, if spaces with dimensions m and n, respectively, combine through the Cartesian product, the resultant space has dimensions $m+n$, whereas if they combine through the tensor product the resultant space has a dimension of mn.

The possibility of linear superposition with tensor product provides a very interesting feature of quantum systems – the ability to interpret the action of separate gates[3] on separate spaces as a single operator on the combined space. As an example, consider two gates: the first one, U_1 takes in two inputs and flips the second input if the first input is $|1\rangle$ [4]; the second gate, U_2, gives the output $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ if the input is $|0\rangle$ and

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

when the input is $|1\rangle$ [5]. We could treat the first gate as an operator on C^4 with the ordered basis set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and represent it by the matrix:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0. \end{pmatrix}$$

Similarly, the second gate could be treated as an operator on C^2 with the basis set $\{|0\rangle, |1\rangle\}$ and be represented by:

$$B = \sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1. \end{pmatrix}$$

We could separately perform the operations on the respective components of $C^4 \otimes C^2$ and then tensor the re-

[3] For now, think of a gate simply as a linear operator on the Hilbert space in which qubits are unit vectors.

[4] Refer to section 8.2.

[5] Refer to section 8.1

sults. Interestingly, however, one could also operate $U_1 \otimes U_2$ on C^8 with the ordered basis $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$, $U_1 \otimes U_2$ being the transform defined by the following matrix:

$$\sqrt{2}\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \end{pmatrix}$$

Note that each entry of the new matrix is a simple scaling of the first matrix A by entries of B.

Another feature, a very powerful one, resulting from the action of linear operations on tensor product spaces, is 'quantum parallel processing' Consider the n-qubit system $|0\rangle \otimes |0\rangle.....|0\rangle$. If we operate U_2 on each qubit of this system, we get

$$|\psi\rangle = \Pi_{i=1}^{n} \otimes B|0\rangle = \frac{1}{2^{n/2}} \Sigma_{x=0}^{2^n-1} |x\rangle.$$

Thus we are able to generate a state containing all the 2^n possible bit combinations with only n elementary operations. Any further operation applied to the resulting superposition acts 'parallelly' on all the elements of the superposition.

5. Entangled States

Consider the two qubit state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, known as the EPR pair. Let us try to express it as a tensor product of two single qubit states. We see that we get a form

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle),$$

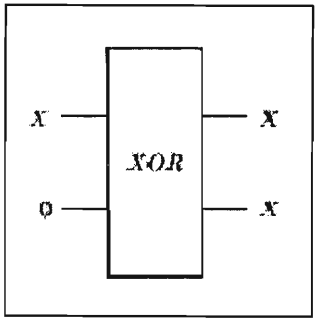
which cannot be the same as the EPR pair for any values of 'a's and 'b's (since $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are the basis states of a 4 dimensional space). Such states, which cannot be split into separate qubits are called entangled states. They cannot be specified by specifying the states of the constituent qubits. These kind of systems have no analogue in the macroscopic world where the description of any system can be broken down into that of its parts. Thus, entangled states defy classical thinking. Another way to look at entangled states is to consider what happens when we make measurements on its bits. On measuring any one of the two qubits in the EPR pair, the other one also collapses to the same measured state. This property is called 'maximum entanglement'. There are other states where a measurement of one qubit does not completely determine the other one, but changes its probabilities of measurement. For example, in the state $\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle)$, if the first qubit is measured and is found to be $|0\rangle$, the probability of measurement of the second qubit as $|1\rangle$ changes from $\frac{2}{3}$ to $\frac{1}{2}$:

$$\frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle) \xrightarrow{\text{1st qubit measured as } |0\rangle}$$

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Therefore, entangled states can also be defined to be those states in which the measurement of one qubit affects the results of measurements of other qubits.

Figure 3. Cloning an arbitrary classical bit.



6. No Cloning Principle

Consider a XOR gate acting on two classical bits as shown in *Figure* 3.

Thus, an arbitrary bit can be duplicated. However, we will now see that such is not the case with qubits. We will show that there exists no unitary transformation U

that can duplicate arbitrary qubits. To prove this, let us assume the contrary, i.e., the existence of U_{cl} which does this. So, for any qubit $|x\rangle$, we have $U_{\text{cl}}|x\rangle = |x\rangle|x\rangle$

For two orthogonal qubits $|x_1\rangle$ and $|x_2\rangle$

$$U_{\text{cl}}|x_1\rangle|0\rangle = |x_1\rangle|x_1\rangle$$

$$U_{\text{cl}}|x_2\rangle|0\rangle = |x_2\rangle|x_2\rangle$$

Now, consider $y = \frac{1}{\sqrt{2}}(|x_1\rangle + |x_2\rangle)$. Since U is a cloning operation

$$U_{\text{cl}}|y\rangle|0\rangle = |y\rangle|y\rangle = (\frac{1}{2})(|x_1\rangle|x_1\rangle + |x_1\rangle|x_2\rangle + |x_2\rangle|x_1\rangle + |x_2\rangle|x_2\rangle) \quad (1)$$

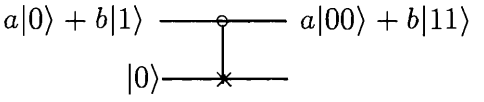
However, by linearity

$$U_{\text{cl}}|y\rangle|0\rangle = (\frac{1}{\sqrt{2}})U_{\text{cl}}(|x_1\rangle|0\rangle + |x_2\rangle|0\rangle) =$$

$$(\frac{1}{\sqrt{2}})(|x_1\rangle|x_1\rangle + |x_2\rangle|x_2\rangle) \quad (2)$$

Since $|x_1\rangle$ and $|x_2\rangle$ are orthogonal, (1) and (2) can not be identical. Hence, our assumption must be wrong and that proves the non-duplicability of arbitrary quantum states.

To understand the fundamental nature of this result, consider the example of an arbitrary control qubit $a|0\rangle + b|1\rangle$ acting on input $|0\rangle$ by a C_{NOT} gate :



The input 2 qubit system can be described as $a|00\rangle + b|10\rangle$. The output is $a|00\rangle + b|11\rangle$, in which both the

[6] Refer to section 5.

qubits are in the same state[6]. If we measure one of the output qubits we get $|0\rangle$ or $|1\rangle$ with probabilities $|a|^2$ and $|b|^2$, respectively. However, this measurement reduces the other qubit also to the state measured. Thus, a measurement on the other qubit does not give any additional 'information' about 'a' or 'b'. So we can see that the information present in the original qubit has not been duplicated. Let us pause here to consider what kinds of cloning are allowed and what kinds are not allowed. A known qubit can be cloned; on the other hand an unknown qubit $a|0\rangle + b|1\rangle$ can only be placed in a superposition of the form $a|00\rangle + b|11\rangle$ (in general, the n qubit entangled state $a|00....0\rangle + b|111....1\rangle$). But it is not possible to achieve a superposition of the form $(a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \otimes ..... \otimes (a|0\rangle + b|1\rangle)$ starting from a single unknown qubit $a|0\rangle + b|1\rangle$.

7. Measurement

A measurement of a quantum system is a disturbance of the system such that the system collapses to one of a set of eigenstates. Thus, every measurement of a quantum system has associated eigenstates. For example if we disturb(i.e. measure) a photon with a vertically polarized filter placed in its path, the two associated eigenstates will be $|\uparrow\rangle$ and its orthogonal state $|\rightarrow\rangle$. A measurement of a single qubit system projects it to either of the two eigenstates. What is important to understand is that once measured the qubit continues to remain in that state, i.e. it continues to give the same measured value, if further measurements are made with respect to the same eigenstates. In the photon example the incident photons will be measured by the polaroid as $|\rightarrow\rangle$ or $|\uparrow\rangle$. The ones measured as $|\uparrow\rangle$ will be allowed to pass through by the polaroid. After this, if a different filter with eigenstates of measurement $|\nearrow\rangle$ and $|\nwarrow\rangle$ is put in the photon's path then it will measure half of these vertically polarized photons as $|\nearrow\rangle$ and the other half as $|\nwarrow\rangle$.

In a multiple qubit system measurement of one or more qubits collapses the system to a superposition compatible with the measured values. For example, if the measurement of the first qubit of the system $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ results in a $|1\rangle$ being measured, the system collapses to

$$\frac{c|10\rangle + d|11\rangle}{\sqrt{c^2 + d^2}}.$$

Note that the coefficients have been renormalized.

In a multiple qubit system measurement of one or more qubits collapses the system to a superposition compatible with the measured values.

8. Quantum Gates: The Dynamics of Qubits

We will represent the transformation of qubits, i.e. the transformations of quantum systems from one state to another as actions of quantum gates. This dynamics is governed by the Schroedinger equation, which implies that the inner product of the underlying space is preserved during any transition between states(i.e., orthogonality is preserved). Linear transformations which preserve orthogonality are called unitary transformations and have the special property that

$$UU^* = I$$

(where U^* is called the adjoint and is the transformation described by $\langle Uv, w\rangle = \langle v, U^*w\rangle$ for every pair of vectors v and w. In a matrix representation, the adjoint is the complex conjugate of the transpose matrix). From this property we can easily see that a unitary transformation will be reversible, the inverse transformation being U^*

We will be representing a gate by specifying the action it performs on the basis states; action on arbitrary qubits can be derived using linearity.

8.1 Single Qubit Gates

Other than identity, the only classical single bit gate is the NOT gate (which flips the state). The quantum

Hadamard gate takes in a qubit in one of the basis states and puts it into a superposition.

analogue of this can be imagined as a 180 degree rotation about the y axis on the qubit sphere. However, rotation by all other angles is also possible, yielding a variety of other gates. Some of these are

1. The identity transformation,

$$I : |0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \longrightarrow |1\rangle$$

2. Negation,

$$X : |0\rangle \longrightarrow |1\rangle$$

$$|1\rangle \longrightarrow |0\rangle$$

3. Phase shift,

$$Z : |0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \longrightarrow -|1\rangle$$

4. A combination of negation and phase shift,

$$Y : |0\rangle \longrightarrow -|1\rangle$$

$$|1\rangle \longrightarrow |0\rangle$$

5. The Walsh–Hadamard transformation,

$$H : |0\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Note particularly the last one of the above transformations, known as the Hadamard gate. It takes in a qubit in one of the basis states and puts it into a superposition. The action by this gate on a set of qubits in their basis states is the first step in many quantum algorithms.

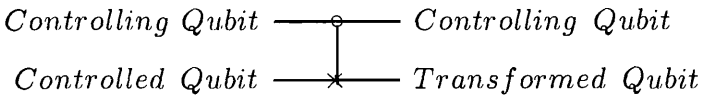
8.2 Multi Bit Gates and the Quantum Computer

All the classical circuits can be synthesized using only the AND and NOT gates.

The most important two bit gate is the C_{NOT} (controlled NOT) gate which acts on two qubits, flipping the second qubit (controlled qubit) if the first qubit (controlling qubit) is $|1\rangle$ and otherwise leaving the second qubit unchanged. The action of the gate can be summarized as:

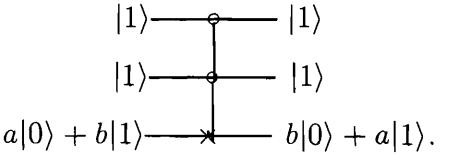
$$|00\rangle \longrightarrow |00\rangle$$
$$|01\rangle \longrightarrow |01\rangle$$
$$|10\rangle \longrightarrow |11\rangle$$
$$|11\rangle \longrightarrow |10\rangle$$

Graphically it is portrayed as



where the circle represents the controlling qubit and the cross, the controlled qubit.

We know that all the classical circuits can be synthesized using only the AND and NOT gates. The classical NOT gate is a reversible gate (being its own inverse). We have an analogous quantum NOT gate. However, we notice that the classical AND gate is a non-reversible gate (a simple check to see whether a gate is reversible is, of course, to try and get back the inputs uniquely given the outputs). So we circumvent the problem by reproducing the inputs at the output, along with the ANDed output. This can be done by using the 3-bit controlled-controlled (or the Toffoli) gate which flips the third input if the first two are both $|1\rangle$. It is graphically represented as:



Using reversible AND and NOT gates, a quantum computer, capable of performing any task a classical computer can perform, can be built.

Using the outer product notation shown in the section on qubits, we can write the Toffoli gate's action as

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\mathrm{NOT}}$$

where the C_{NOT} itself can be broken into simpler gates as

$$C_{\mathrm{NOT}} = |0\rangle\langle 0| \otimes I + |1\rangle|1\rangle \otimes X.$$

Thus, we have

$$T = |0\rangle\langle 0| \otimes I \otimes I + (|1\rangle\langle 1|) \otimes (|0\rangle\langle 0|) \otimes I +$$

$$(|1\rangle\langle 1|) \otimes (|1\rangle\langle 1|) \otimes X.$$

Though slightly out of place, it would be instructive to pause here to look at what all this notation means. $|0\rangle\langle 0|$ is the transform that takes $|0\rangle$ to $|0\rangle$ and $|1\rangle$ to $(0,0)^T$ So the first term in the expression for T acts on the first bit by changing it to the scalar 0 if it is $|1\rangle$ and leaving it unchanged if it is $|0\rangle$. The second and third bits are left unaffected. The net result is that the first term leaves the three qubit set unchanged if the first qubit is $|0\rangle$ and changes it to the scalar 0 if the first bit is $|1\rangle$. The other two terms can be understood similarly ($|1\rangle\langle 1|$ being the transform which converts $|0\rangle$ to the scalar 0 and leaves $|1\rangle$ unchanged). As an example, consider the action of the Toffoli gate on $|110\rangle$. The first and the second terms in the expression gives the scalar 0 as output. The third term gives $|111\rangle$. The overall result, as you can deduce, is

$$T|110\rangle \longrightarrow |111\rangle,$$

which fits in with our earlier description of the gate.

We can construct a reversible AND gate by acting with the Toffoli gate on $|x, y, 0\rangle$.

$$T|x, y, 0\rangle \longrightarrow |x, y, xANDy\rangle.$$

Having reversible AND and NOT gates in our possession, we can realize any Boolean function by using arrays

of these gates (i.e., a quantum computer, capable of performing any task a classical computer can perform, can be built). What we have seen already is good enough to perform the tasks any existing computer can. As we shall see in the second part of this article, there is a lot more that a quantum computer can do.

9. Conclusion

In this article we have seen how the principles of quantum physics can be exploited in making a computational device. However, we still haven't seen the kind of algorithms a quantum computer would use and how they would be different from traditional algorithms. We will look at these issues in the next part of this article, with the help of Shor's famous factorization algorithm. We will also briefly mention some practical issues and the progress achieved so far.

Suggested Reading

[1] S Lloyd, *Scientific American*, Oct 1995.
[2] N Gershenfeld and I L Chuang, *Scientific American*, Jun 1998.
[3] D P Divincenzo, *Science*, Vol. 270. Oct 13, 1995.
[4] Online resources at http://www.qubit.org/
[5] Online resources at http://xxx.lanl.gov/archive/quant-ph/

Address for Correspondence
C S Vijay
hostel 9, IIT, Powai
Mumbai 400 076, India.
Email:csvijay@ee.iitb.ernet.in

Vishal Gupta
Herald Logic Inc
IT Business Incubator
Department of Physics
IIT Powai,
Mumbai 400 076, India.
Email: gupta_vish@yahoo.com

"When the theory (evolution by natural selection) was first put forward, by far the vaguest element in its composition was the principle of inheritance. No man of learning or experience could deny this principle, yet, at the time, no approach could be given to an exact account of its working. That an independent study of Natural Selection is now possible is principally due to the great advance which our generation has seen in the science of genetics. It deserves notice that the first decisive experiments which opened out in biology this field of exact study, were due to a young mathematician, Gregor Mendel, whose statistical interests extended to the physical and biological sciences."

R A Fisher, 1930