How to Visualize a Matrix

BY (b)(3)-P.L. 86-36

Unclassified

Since we shall be talking about matrices and vectors, let us begin by saying what we mean by those words:

A vector is an ordered sequence of numbers which obeys certain rules of addition and multiplication; for instance, (3, 7, 2) is a vector if it obeys certain rules of combination. Notice that (3, 7, 2) is *not* the same as (7, 3, 2) or (2, 3, 7). These are three different vectors.

A matrix is a two-dimensional ordered array of numbers which obeys certain rules of addition and multiplication; for instance,

$$\begin{vmatrix} 3 & 2 \\ 5 & 1 \end{vmatrix}$$

is a matrix if it obeys certain rules of combination.

When stated in this way, the definitions sound rather arbitrary. An ordered sequence of numbers sounds like an abstract and high-brow idea. Actually, this is not true; we are all familiar with ordered sequences of numbers.

Example 1.—What would you understand by the ordered sequence of three numbers 12–25–63? That's right, it is Christmas of this year, in the "civilian" system of month, day, year. ("Militarily," it would be 25–12–63).

Example 2.—What would you understand by the ordered sequence of three numbers 202–772–8956? It is a telephone number in long-distance dialing. The first number, 202, indicates the Washington area; the 772 is the exchange; and 8956 is the individual's phone number.

Example 3.—What would you understand by 53–65–13–29.50? That is a weather report. If you dial the weather-forecast number, you will be told the temperature, the relative humidity, the wind-velocity, and the barometric pressure, in that order. The voice on the phone tells you which is which; but if you were sending this information at expensive cable rates, you would send only the numbers.

Example 4.—From cryptography, we have examples like this:

Letter of alphabet	A	B	C	D	Z
Number of occurrences in 1,000 letters	70	20	35	36	2

These 26 numbers could be written as an ordered sequence, (70, 20, 35, . . . 2) without mentioning the letters of the alphabet. We would understand that the first number, 70, was the number of A's; the next, the number of B's, and so on.

Example 5. Suppose we made a similar count of frequencies of letters of the alphabet on 1,000 letters each day for a month in this fashion:

Letter of the Alphabet

Date	A	B	C	D	. . . . .	Z
Nov. 1	70	20	35	36	. . . . .	2
2	69	19	31	33	. . . . .	1
3	75	21	30	31	. . . . .	3
.	.	.	.	.	. . . . .	.
.	.	.	.	.	. . . . .	.
30	65	15	35	30	. . . .	0

Inside the "box" we have a two-dimensional array which is "ordered." We know that the n^{th} row refers to the n^{th} day of the month, and the n^{th} column refers to the n^{th} letter of the alphabet. This is a 30-by 26 array.

We have not called this two-dimensional array a matrix, because it is not a matrix yet. Neither is the row (70, 20, 35, . . . 2) of the previous example a vector—not yet. These ordered arrays of numbers become matrices, or vectors, when they satisfy certain requirements about how they combine with one another. Here are the rules:

(1) "Vectors Add Component by Component." Each one of the numbers that make up a vector, like the 3 of (3, 2, 7) is a "component;" (3, 2, 7) has three components. To add two vectors, we add the first component of one vector to the first component of the other vector, and the result is the first component of the sum vector; so also for the other components. In symbols this is

$$(3, 2, 7) + (1, 2, 3) = (4, 4, 10)$$

because

$$(3 + 1 = 4, \text{ etc.})$$

and in general

$$(a, b, c) + (x, y, z) = (a + x, b + y, c + z)$$

To multiply a vector by a scalar—a "scalar" is an ordinary number—we multiply each component by the scalar. For instance:

$$2(3, 2, 7) = (6, 4, 14).$$

That is what we would naturally expect. Two times a vector means that we take the vector twice, so that $2(3, 2, 7) = (3, 2, 7) + (3, 2, 7) = (6, 4, 14)$. In general, $a(x, y, z) = (ax, ay, az)$.

To multiply two vectors together, we multiply corresponding components and add the results. The product of two vectors is therefore a scalar, or ordinary number. For instance:

$$(3, 2, 7) \cdot (1, 2, 3) = 3{\cdot}1 + 2{\cdot}2 + 7{\cdot}3 = 3 + 4 + 21 = 28.$$

All these rules for addition and multiplication agree with the interpretation of (x, y, z) as the coordinates of a point. In two dimensions we write (3, 1), for instance, for the coordinates of this point:

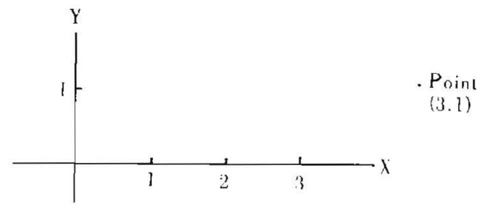


Fig. 1.

The ordered sequence of two numbers (3, 1) indicates the point where $x = 3$ and $y = 1$. The first number always is the value of x and the second is the value of y, by a standard convention. The vector (3, 1) tells us to go 3 units of distance to the right and then 1 unit up. Another way to indicate this point is to use an arrow which starts at the origin and ends at the point, like this:

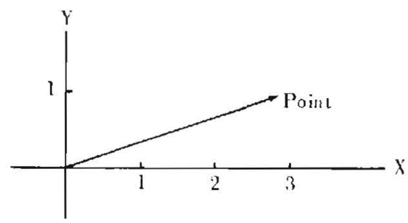


Fig. 2.

We would call this arrow the vector v if we had previously specified the length and the direction of the arrow. Then $v = (3, 1)$, and we say that the vector v, thought of as a certain distance in a certain direction, has been "expressed in terms of its components, (3, 1)." When we add two "arrows," or directed quantities, we do it by putting the beginning of one arrow at the end of the other and connecting the new end-point to the origin, in this fashion:

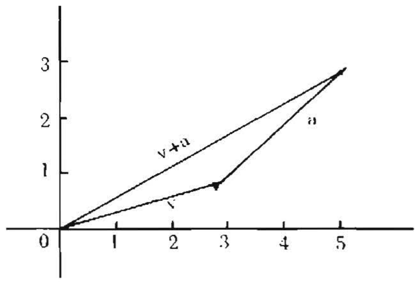


Fig. 3.

As the Fig. shows, the vector **a** is 2 units to the right and 2 units up. The components of **a** are (2, 2). The sum $v + a$, which goes to the "total" point, has components (5, 3). So we have $(3, 1) + (2, 2) = (5, 3)$. This agrees with the rule for addition of vectors that we expressed above, namely, "add corresponding components to find the corresponding component of the sum." In particular, if we add a vector to itself, we double each component:

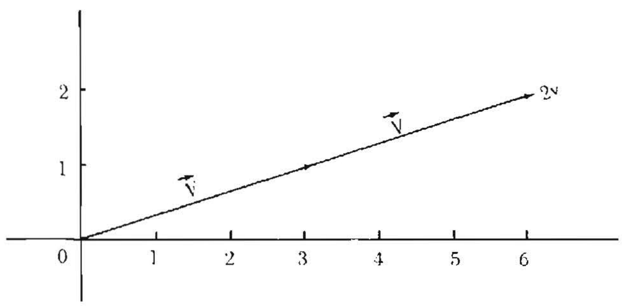


Fig. 4.

Notice that multiplying a vector by 2 has doubled its length but has *not* changed its direction. The direction is still unchanged when we multiply by any scalar:

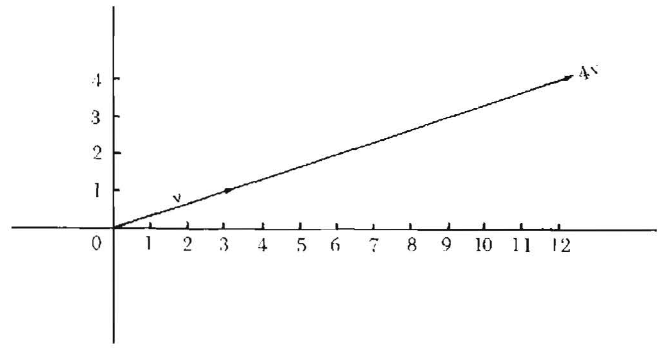


Fig. 5.

In most applications, particularly the applications that we shall make here, the direction of a vector is more important than its length. If we write v for any vector and a for any scalar, or ordinary number, then **av** is essentially the same as v, for many purposes. In fact, when we divide a vector by its own length, so that we have a vector of length 1 in the same direction, we say that we have "normalized" the vector. The idea is that it is still essentially the same vector; it has merely been reduced to a standard form.

Multiplying two vectors we defined above as multiplying corresponding components and adding the results, that is,

$$(a, b, c) \cdot (x, y, z) = ax + by + cx \text{— a scalar quantity.}$$

How does this fit in with our picture of vectors as arrows? First consider the special case of multiplying a vector by itself:

$$(a, b, c) \cdot (a, b, c) = a^2 + b^2 + c^2$$

In two dimensions this is $(a, b) \cdot (a, b) = a^2 + b^2$.

The arrow is the hypotenuse of a right triangle. By geometry, the square of the hypotenuse equals the sum of squares of the other two sides, so that if we measured the lengths of the lines in the picture we would find that, physically, $v^2 = a^2 + b^2$. If we did the same thing in three dimension, we would find that the lengths of the lines drawn

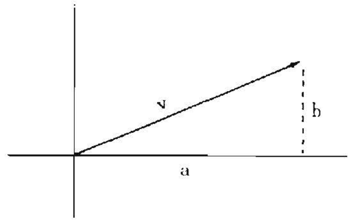
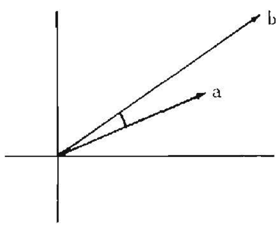


Fig. 6.

would agree with $v^2 = a^2 + b^2 + c^2$. Our definition, then, of multiplying by adding products of components agrees with the geometry of the picture.

When two different vectors are multiplied together, we can reasonably expect the result to depend on the lengths of both vectors and on the directions of both. The conventional definition is such that the product of two vectors depends on the product of the two lengths, and it depends on their directions because it depends on the angle between them:



$\vec{a} \cdot \vec{b}$

(length of $\vec{a}$) (length of $\vec{b}$) $\cos\theta$

Fig. 7.

In our applications we shall limit ourselves almost entirely to the special case where one of the vectors is of unit length. Call the one of unit length **u** and the other one **a**. Then we have

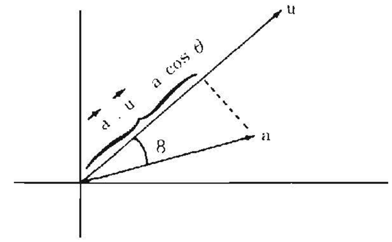


Fig. 8.

By the definition of the cosine, the length of the projection of **a** on **u** is **a** cos θ where **a** = length of **a**. When **a** is greater than 1, this is still true, but we must extend **u** in order to draw the projection in this manner:

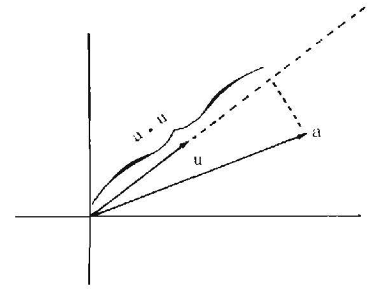


Fig. 9.

Perhaps it should be mentioned here that these ideas are not limited to the study of geometrical figures. We all know that a graph can have many different meanings. A curve or a jagged straight line sometimes indicates the behavior of the stock market from week to week; sometimes it indicates daily temperatures or something else about the weather; and there are many other possibilities. The meaning we are interested in here is one that is related to cryptography. In a few minutes, we shall define this in detail.

First, we must say a little about the two-dimensional arrays, or matrices. The example cited previously (p. 32) had 26 columns and 30 rows. When the number of rows is the same as the number of columns, we have a "square" matrix. These are the easiest to work with, and they are enough for our purposes now, so we shall talk from now on about square matrices.

The rule for adding two matrices together is the same as that for vectors, namely, "add corresponding components to get the corresponding component of the sum." For instance, in 2-by-2 matrices we may have:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} x & y \\ z & w \end{vmatrix} = \begin{vmatrix} a+x & b+y \\ c+z & d+w \end{vmatrix}$$

The rule for multiplying by scalars is the same as for vectors – "multiply each component by the scalar." For instance,

$$a \begin{vmatrix} x & y \\ z & w \end{vmatrix} = \begin{vmatrix} ax & ay \\ az & aw \end{vmatrix}$$

The rule for multiplying two matrices together is based on the rule for multiplying two vectors together, but that rule has to be applied several times. To state the rule, we first think of a matrix as a set of vectors. Row 1 of the *abcd* matrix, above, is (a, b), which we can call the vector $\mathbf{r}_1$ ("row one"). The second row is (c, d), which we call $\mathbf{r}_2$. In the *xyzw* matrix, column 1 is a vector written as a column, so we call it $c_1' = \begin{vmatrix} x \\ z \end{vmatrix}$, and likewise $c_2' = \begin{vmatrix} y \\ w \end{vmatrix}$. We have written primes on the *c's* to remind us that these are columns of the second matrix, not the first. Then the rule for matrix multiplication is

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} \cdot \begin{vmatrix} x & y \\ z & w \end{vmatrix} = \begin{vmatrix} r_1 \\ r_2 \end{vmatrix} \cdot (c_1', c_2') = \begin{vmatrix} r_1 \cdot c_1' & r_1 \cdot c_2' \\ r_2 \cdot c_1' & r_2 \cdot c_2' \end{vmatrix}.$$

That is, to get the element on the *first* row and the *second* column of the product, we multiply the first row (of the *abcd* matrix) by the second column (of the *xyzw* matrix). For 3-by-3 matrices or larger we simply extend the definition:

(b)(3)-P.L. 86-36

$$\begin{vmatrix} r_1 \\ r_2 \\ r_3 \\ \cdot \\ \cdot \\ \cdot \end{vmatrix} (c_1', c_2', c_3' \ldots) = \begin{vmatrix} r_1 \cdot c_1' & r_1 \cdot c_2' & r_1 \cdot c_3' \ldots \\ r_2 \cdot c_1' & r_2 \cdot c_2' & r_2 \cdot c_3' \ldots \\ r_3 \cdot c_1' & r_3 \cdot c_2' & r_3 \cdot c_3' \ldots \\ \cdots & \cdots & \cdots \end{vmatrix}$$

Notice that it is reasonable to call these rows and columns "vectors," because they are added together and they are multiplied by scalars according to the vector rule. To see this in detail, let us write c_1 and c_2 without primes for the columns of the *abcd* matrix and r_1', r_2' with primes for the rows of the *xyzw* matrix. Then the rule for addition of matrices becomes:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} x & y \\ z & w \end{vmatrix} = \begin{vmatrix} r_1 \\ r_2 \end{vmatrix} + \begin{vmatrix} r_1' \\ r_2' \end{vmatrix} = \begin{vmatrix} r_1 + r_1' \\ r_2 + r_2' \end{vmatrix}$$

This agrees with the rule for vector addition. We also find that vector multiplication and matrix multiplication agree when we write the first matrix as (c_1, c_2) and the second one as (c_1', c_2').

Scalar multiplication of matrices is done by multiplying each component of the matrix by the scalar. This agrees with vectors multiplied by scalars:

$$s \begin{vmatrix} r_1 \\ r_2 \end{vmatrix} = \begin{vmatrix} sr_1 \\ sr_2 \end{vmatrix} \text{ and } s\,(c_1, c_2) = (sc_1, sc_2), \text{ where } s = \text{scalar.}$$

In this way we see that we can think of a matrix as a set of vectors, if we wish. This will be particularly useful in the special case of a matrix multiplied by a vector, in that order, such as

$$\begin{vmatrix} 3 & 2 \\ 1 & 5 \end{vmatrix} \begin{vmatrix} 4 \\ 6 \end{vmatrix} = \begin{vmatrix} 3 \times 4 + 2 \times 6 \\ 1 \times 4 + 5 \times 6 \end{vmatrix} = \begin{vmatrix} 24 \\ 34 \end{vmatrix}$$

The vector $\begin{vmatrix} 4 \\ 6 \end{vmatrix}$ has been changed, by multiplication, into the vector

$$\begin{vmatrix} 24 \\ 34 \end{vmatrix}$$

We can write this in vector form as

$$\begin{vmatrix} r_1 \\ r_2 \end{vmatrix} (c') = \begin{vmatrix} r_1 \cdot c' \\ r_2 \cdot c' \end{vmatrix}$$

Now let us *draw* a matrix as a set of vectors. Using the matrix just mentioned we have

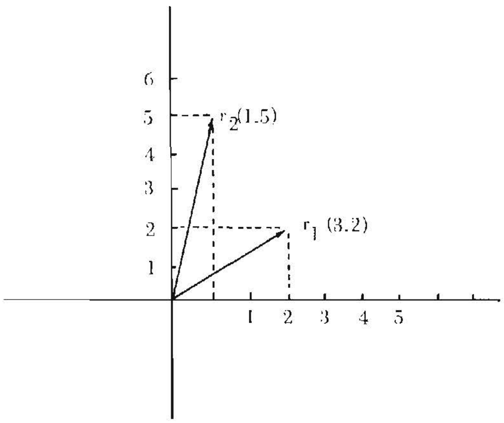


Fig. 10.

The matrix is represented by the two arrows, taken in the order 1, 2. The same arrows taken in the order 2, 1 would represent the matrix

$$\begin{vmatrix} 1 & 5 \\ 3 & 2 \end{vmatrix}$$

which is a different matrix because the rows have been interchanged. To avoid trouble, we shall consider only a problem in which the order of the rows makes no difference. Then we can think of the set of n arrows as representing an n-by-n matrix. Of course, this has to be done in an n-dimensional space.

In case anyone objects to the idea of a many-dimensional space, perhaps I should mention that it is only a convenient way of speaking. We all know that graphs are a help in exhibiting numerical facts. When we want to represent a single number, we can mark off a distance on a line:

When we want to an represent ordered pair, we draw another line at right angles to this one and plot the two numbers as we did before, so (3.1) is

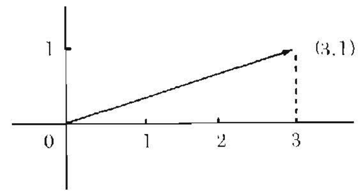


Fig. 11.

To represent an ordered triple, such as (3, 1, 4) we draw a third line at right angles to both of those. This may be shown as:

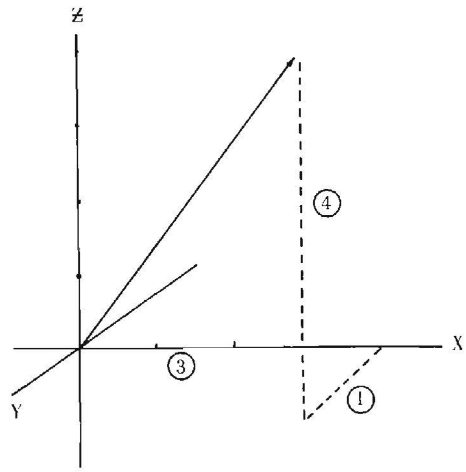


Fig. 12.

Now we cannot draw any more lines at right angles to all of these three axes, because we live in a three-dimensional physical world. What we can do is to say, in effect, "and so on." We can visualize one, two and three dimensions. We then assume that similar things will be true in other dimensions, and we form a vague mental picture of axes and points. This is not mathematically wrong, in spite of the vagueness, because the mathematics is in the written equations. The mental picture, though vague and incomplete, is a help in the same way that an ordinary graph is a help in grasping all at once the facts that are stated more exactly in a table of numbers.

To get back to our matrices: when we multiply a vector, say v, by a matrix M, the result Mv is another vector. Multiplying v by M has changed v into a new vector. Here is an example. We take the vector, with two components,

$$\mathbf{v} = \begin{vmatrix} 1/\sqrt{5} \\ 2/\sqrt{5} \end{vmatrix}$$

We chose the inconvenient factors, $\sqrt{5}$, because it makes the vector have unit length. Let us change the vector by multiplying it by the matrix

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix}$$

Then $M\,v$ will be a new vector. This diagram shows the matrix represented by the two arrows marked 1 and 2, meaning the first row and the second row respectively. The original vector, v is the short vector between 1 and 2. The result, M v, is marked by the asterisk. (See Fig. 13).

This resultant vector, Mv, is longer than the unit vector, v, but is almost in the same direction. If we keep the matrix 1, 2 constant and vary the direction of v, we can find a direction such that Mv is *exactly* in the same direction as **v**. In the case of the matrix which we used previously, namely,

$$M = \begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix},$$

U is such a vector. (See Fig. 14, page 44).

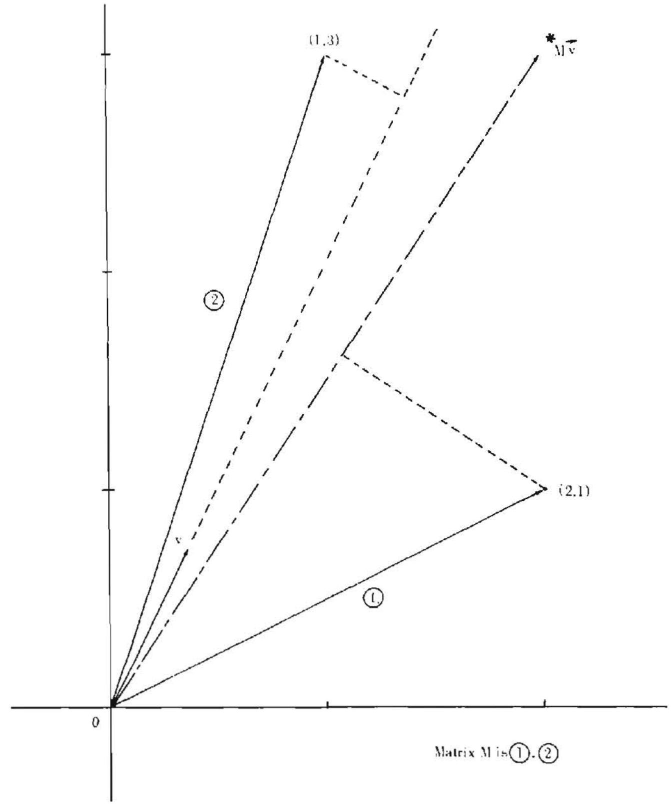


Fig. 13.

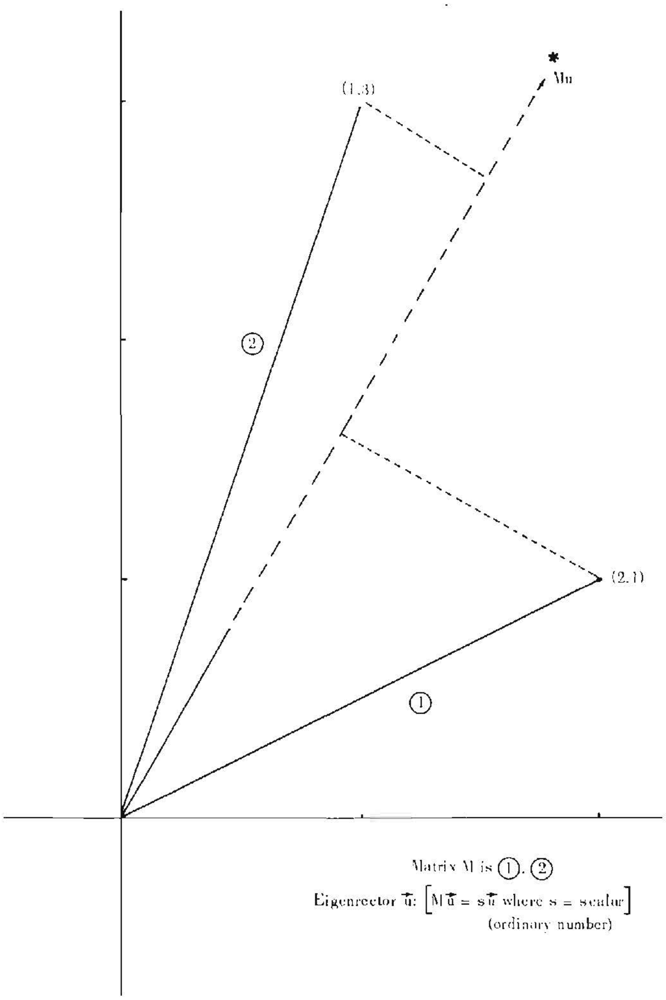


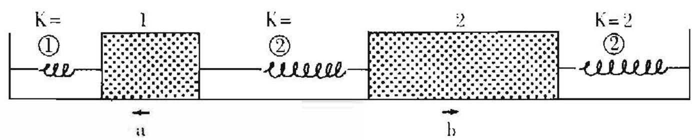
Fig. 14.

M **u** is in the same direction as **u**, but it is longer by a factor of 3.6, approximately. This ratio, 3.6, is the "eigenvalue." When the original vector is of unit length, as u was, then the eigenvalue is the length of Mu.

This vector **u** is one of the "eigenvectors" or "characteristic vectors" of the matrix. Every eigenvector is a vector, but it is an eigenvector, or characteristic vector, only with respect to a certain matrix, or matrices, of which it is characteristic. "Eigen" in German means "proper" or "belonging to," in this sense. Usually a matrix which has n rows and n columns also has n eigenvectors, each with its own eigenvalue (increase in length). The matrix $\begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix}$ has the eigenvector (.526, .851) with eigenvalue 3.62, shown in Fig. 2, and a second one, (.851, .526) with eigenvalue 1.382, not shown.

A natural question to ask is, Do these eigenvectors and eigenvalues have any practical use? From the diagram they look like a mathematical freak. The vector **u** happens to be pointed in just the right direction so that when we multiply it by M it is still in the same direction. Is this anything more than a coincidence?

The answer is, Yes. These special vectors have physical meaning and practical uses. The most concrete interpretations occur in physics, where the elements of the matrix are usually not numbers but differential operators. We can write D to mean "differentiate with respect to time, t," and D^2 to mean "differentiate twice," and so on. Then the forces acting on a set of physical objects will be given by several equations in which the variables are coordinates representing the positions of various objects, and these are shown with powers of D before them. So we can write a matrix involving powers of D and ordinary numbers. The eigenvectors of this matrix will describe certain important features of the motion of the system in which the eigenvectors will be parameters. For instance, suppose we have two weights, of mass 1 kg and 2 kg, which slide without friction on a horizontal surface; and suppose these weights are attached to springs in this way:



K=strength of spring

Fig. 15.

We hold weight 1 in its rest position, a centimeters to the left, and weight 2 in the same way, b centimeters to the right, and we release them. If we choose a and b at random, the weights will move to and fro in an irregular, complicated, and continuous manner. But if we choose a and b correctly (in fact the correct choice is $a = 1$ centimeter to the left and $b = 1$ centimeter to the right) they will vibrate in a simple, regular way, like this:

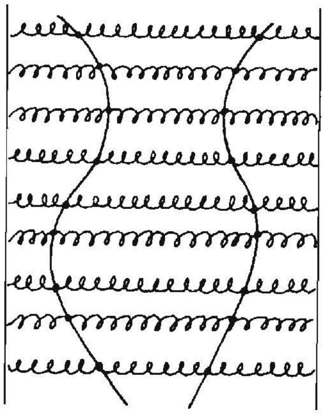


Fig. 16.

The equations representing the force exerted by the springs at each time, t, and the resulting displacements of the two masses can be written as a matrix involving the time-derivative D:

$$\begin{vmatrix} D^2 + 3 & -2 \\ -2 & 2D^2 + 4 \end{vmatrix} \begin{vmatrix} x_1 \\ x_2 \end{vmatrix} = 0$$

where x_1 and x_2 are respectively the displacements, to the right, of mass 1 and of mass 2. The eigenvectors, also called eigenfunctions in such problems, of this matrix are functions of time which describe the mode of vibration pictured above, and a similar but different mode, not shown. The eigenvalues are the corresponding frequencies of vibration. Similar situations, but more complicated, are of great practical importance. For instance, instead of the two sliding weights we may have two heavy fixtures on a ship, connected by metal beams with some degree of flexibility. If this system has a mode of vibration with a frequency equal to the natural frequency

of typical waves of the ocean, then a storm could set up a steady vibration that might build up to the point of being dangerous. Ship designers have to avoid structures with that frequency of vibration. Likewise, in airplane design, vibration analysis is carefully studied by specialists.

One application to cryptanalysis is as follows. We start with some set of frequency counts, such as the frequencies of different letters of the alphabet at different positions in the cipher text, or something like that. From these counts we drive a set of columns of figures. How this is done depends on the nature of the cipher we are studying. We compare these columns in pairs to see whether or not they seem to be different versions of the same "ideal" column and differ only in random fluctuations. If there is a probability p that columns i and j are alike, then the probability is also p that column j is like column i. We can write this as $p_{ij} = p_{ji}$. If we write these p's with i as row heading and j as column heading, we have a symmetrical matrix. A very simple example is this:

1	$p_{11} = 1.000$	$p_{12} = .050$	$p_{13} = .975$
2	$p_{21} = .050$	$p_{22} = 1.000$	$p_{23} = .007$
3	$p_{31} = .975$	$p_{32} = .007$	$p_{33} = 1.000$

(Notice symmetry)

The array of 9 numbers is a square matrix. It can be plotted in 3-dimensional space as a set of 3 vectors, as we did before. Each vector would represent a row of the matrix, or it could represent a column if we prefer, because of the symmetry. In practical cases, the matrix would have more than 3 rows and columns; in fact 30-by-30 would be more typical than 3-by-3. Also the elements would not all be very close to 1 or very close to 0; they could have any value in between.

In this large matrix some columns would be similar to one another. The remaining columns would all be approximately inverses or opposites of the first set of columns, like this:

ALIKE

.9	0	.9	.9
0	.9	0	0
.7	0	.9	.9
.9	0	.7	.9

OPPOSITE

Plot this in 4-dimensional space, each column being one point. The points representing the first, third, and fourth columns will be close together. The point representing the second column will be far away. If there were other columns like column 2, they would be close together but all separated from the set consisting of columns 1, 3, and 4. We would have two clusters of points. We must separate these clusters; in cases where the two types are not very obviously different the separation is difficult. In fact, what we want to do is to find the approximate center of each cluster. These centers will be close to the two ideal points that represent the two ideal types of columns, one the inverse of the other, of which the actual columns are approximate versions. To accomplish this separation, we first make a change of origin, that is, we decide to measure all distances from the center of gravity of all the points. In the example, this center would be close to (1/2, 1/2, 1/2, 1/2). The two clusters are on opposite sides of this center of gravity, and we wish to find a line which will go through the center of gravity and will also pass through the approximate centers of the clusters. Here is a simplified figure, in two dimensions, which is merely suggestive, of course:

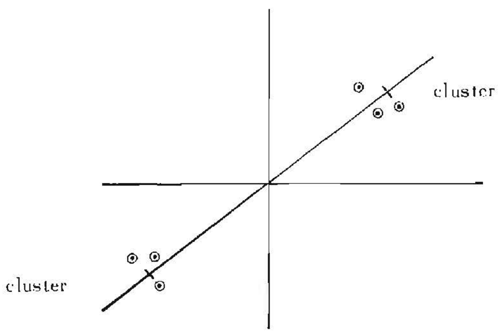


Fig. 17.

It is sufficient to find the direction of this line, rather than the actual centers of the clusters, because the direction of the vector is more important than its length. In fact, in this case we know the length before we start; it will be $\sqrt{n}$ for n points in n dimensions. So we rotate the line, letting it pass through the origin all the time, until we find the best position. We shall define the best position, where it "goes through the clusters" in a sense, as being that position in which the sum of the squares of the projections has the greatest value—a "projection" being the projection of one of the points onto the line:

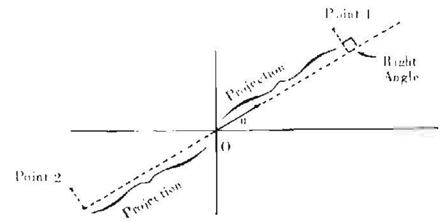


Fig. 18.

From each point we drop a perpendicular to the line; from the point where this perpendicular meets the line to the origin 0 is a segment of the line called the projection of the point. We do this for all points in both clusters. We square the numbers representing the lengths of the projections in order to get rid of minus signs, and then we add these squares. To indicate the position of the line, we use a vector **u** of unit length, in that direction.

In a geometrical picture, how do we usually represent the sum of squares of numbers? We do it by drawing the numbers as sides of a right triangle. The square of the length of the hypotenuse is equal to the sum of the squares of the other two sides. We saw it previously in two dimensions. In three dimensions it still holds as a sum of 3 squares:

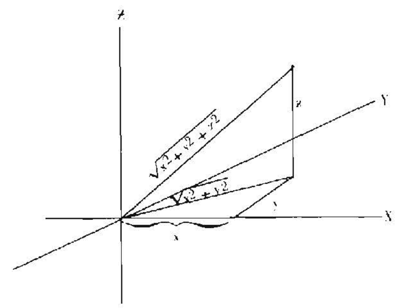


Fig. 19.

In more than 3 dimensions we cannot draw the picture, but the idea remains valid. Notice that it makes no difference which number we mention first; so also, it makes no difference which axis we call x and which one, y; $x^2 + y^2 + z^2 = y^2 + z^2 + x^2$, etc.

In the example we are considering, we wish to draw a picture representing the sum of the squares of the "projections" mentioned above. We must use each of the projections as a side of a right triangle. To draw this, we rotate the projections onto the axis, one projection to each axis in any order, thus:

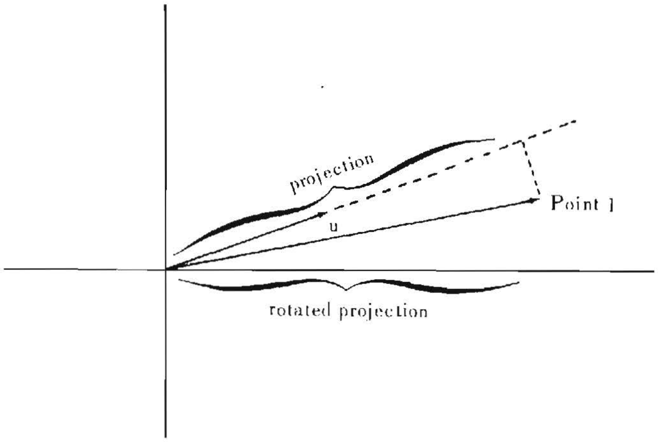


Fig. 20.

These segments on the axis—the rotated projections—are the sides of right triangles, because the axes are at right angles to one another. Then the "hypotenuse" or diagonal, the hypotenuse of the last triangle, represents the sum of the squares that we desire. It is the longest diagonal, from the origin to the farthest corner, of a rectangular box whose sides are these rotated projections. The farthest corner is the only one that does not lie in any coordinate plane.

Now it is a fact that this diagonal of the box, when we think of it as a vector from the origin, is what we had before when we multiplied a vector by a matrix in the form M **v**. As indicated before, multiplication by M changes v into the new vector M **v**, which is the diagonal. The matrix M was represented by a set of n vectors, one vector standing for each row of the matrix. Now we have a given matrix, whose rows (or columns) are the points of the two

clusters. So we do this: we set up a matrix M by using the coordinates of the given cluster-points. If these points are $p_1, p_2, \ldots,$ then M is

$$M = \begin{vmatrix} p_1 \\ p_2 \\ \cdot \\ \cdot \end{vmatrix} \text{ a square matrix.}$$

To find the best postion of **u**, meaning the position that maximizes the sum of the squares of the projections, we leave M fixed and vary **u** by rotating it. We wish to maximize the length of the vector M **u** by varying **u**. Instead, we may just as well say that we wish to maximize the *square* of this length, because the square of a positive number is greatest when the number itself is greatest, and vice versa.

What is the square of the length of any vector, say, the vector **a**? In terms of its components this vector is, say, (a_1, a_2, a_3), and the square of its length was shown before to be $a_1^2 + a_2^2 + a_3^2$. We can write this in matrix form as:

$$\text{Length squared} = (a_1, a_2, a_3) \begin{vmatrix} a_1 \\ a_2 \\ a_3 \end{vmatrix} = a_1^2 + a_2^2 + a_3^2$$

When **a** is written as a vertical column, then the row form of the same components is **a** as a row, called "**a** transpose," and vice versa. The transpose of any matrix, or vector, is formed from the matrix or vector by writing down instead of across, so that rows become columns and columns become rows, as in:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} \text{ transpose } \begin{vmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{vmatrix}$$

The square of the length of any vector a can be written than as "**a** times **a** transpose," which is in symbols $a^T a$. Then the square of the length of Mu is $(Mu)^T Mu$. It can easily be shown that the transpose of a matrix product is the product of the transposes taken in reversed order; in symbols, $(Mu)^T = u^T M^T$. So the square of the length that we wish to maximize is $u^T M^T Mu$. A symmetric matrix is the same as its own transpose, because rows equal columns in symmetric matrices: $M^T = M$ when M is symmetric, as here. So the quality we wish to maximize is $u^T M^2 u$. Of course, M^2 is simply another matrix like M, also of n rows and n columns. We ask, what vector, u, will make $u^T M^2 u$ have its greatest value?

The answer is, the desired value of **u** is the eigenvector of M^2 that goes with its largest eigenvalue. The n-by-n matrix M^2 normally has n eigenvectors and n eigenvalues, one eigenvector for each eigenvalue. If we find all the eigenvalues of M^2, pick the one that is algebraically largest, and find the corresponding eigenvector, say $\mathbf{e}_1$, then that e_1 is the desired value for u. It maximizes the expression we had before: $e_1 M^2 e_1$ is larger than $u^T M^2 u$ for every u other than $\mathbf{e}_1$.

This maximizing property is true for any matrix, say A. If $\mathbf{e}_1$ denotes the so-called "principal" eigenvector of A, meaning the one corresponding to the largest eigenvalue, then $e_1^T A e_1$ is larger than any $\mathbf{x}^T A$ x, where x is a vector other than $\mathbf{e}_1$. The distinguished mathematician Courant proved in a general form, that we can define all the eigenvectors and eigenvalues of any matrix A as the vectors that maximize $x^T A x$, in a certain sense, and their corresponding eigenvalues. That is, we can define eigenvectors and eigenvalues without using the equation $A x =$ (scalar) x; instead, we maximize $x^T A x$.

The conclusion is this. We can find the best position of the vector **u**—the position in which it goes approximately through the centers of the clusters—by finding the eigenvector corresponding to the largest eigenvalue of M^2, which is often called the "principal" eigenvector" of M^2. Now the principal eigenvector of M^2 may be also the principal eigenvector of M itself, because we can take the definition of eigenvector

$$M u = s u \qquad \text{(where } s \text{ is a scalar)}$$

and multiply by M:

$$M^2 u = M (s u) = s (Mu) = s (s u) = s^2 u.$$

That is, every eigenvector of M is also an eigenvector of M^2, and each has n eigenvectors, which are usually distinct. The eigenvalues of M^2 are the squares of the eigenvalues of M. When the eigenvalues of M are all positive, the algebraically largest one of M is also the largest one of M^2, or rather its square is. The square of the principal eigenvalue of M is also the principal eigenvalue of M^2 if some are negative, but the negative ones do not exceed the principal eigenvalue in absolute value. This last situation happens to be the one usually realized in the cryptanalytic problem that gave rise to this discussion, so it is sufficient to find the principal eigenvector of M instead of

M^2. When that is not the case, we could, of course, find the eigenvectors of M^2 with a little more work, but actually this is unnecessary. A different argument shows that it is still sufficient to find the principal eigenvector of M itself.

How we go about calculating eigenvectors and eigenvalues of a given matrix is an extensive question in itself. For the moment, we can say simply that a good many methods are known, some of which are better than others in particular situations. A survey for four of the best methods for general use, and some special methods for use in the National Security Agency, may be found in my paper on the calculation of eigenvectors and eigenvalues.*

* [redacted] (b)(3)-P.L. 86-36 "*Computation of Eigenvalues and Eigenvectors,*" Office of Cryptology, 27 October 1962.