New Applications of Algebra

A mathematician solves some typical, practical, present-day problems — and thereby proves that algebra is doing better than holding its own in modern technology.

by Marshall Hall, Jr.

A friend of mine has observed that there are certain "OK words" whose use imparts a favorable impression. With this in mind he has written a book about computers called *Dynamic Programming*, since the word "dynamic" is filled with all kinds of desirable connotations. I shall take my cue from him and begin with "Algebra of the Space Age," since an application to "space" provides status and modernity to anything so dignified.

Signals coming back to earth from a satellite will be a succession of dots and dashes which we may represent algebraically by a succession of zeros and ones. It is to be expected that reception of a signal coming from millions of miles away will not be perfect. Nevertheless, if the different words produced differ from each other sufficiently, an error in reception of one or two dots or dashes in a word will still leave the receiver with no question as to which the original word was. This is known as the problem of constructing "error-correcting codes" and has been studied extensively.

An example of such a code is the following set of 24 words, each consisting of 12 zeros or ones, with the property that any two of the words differ in at least 6 of the 12 places:

Column number	∞	*0*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
W_1:	1	1	1	1	1	1	1	1	1	1	1	1
W_2:	1	0	1	0	1	1	1	0	0	0	1	0
W_3:	1	0	0	1	0	1	1	1	0	0	0	1
W_4:	1	1	0	0	1	0	1	1	1	0	0	0
W_5:	1	0	1	0	0	1	0	1	1	1	0	0
W_6:	1	0	0	1	0	0	1	0	1	1	1	0
W_7.	1	0	0	0	1	0	0	1	0	1	1	1
W_8:	1	1	0	0	0	1	0	0	1	0	1	1
W_9:	1	1	1	0	0	0	1	0	0	1	0	1
W_{10}:	1	1	1	1	0	0	0	1	0	0	1	0
W_{11}:	1	0	1	1	1	0	0	0	1	0	0	1
W_{12}:	1	1	0	1	1	1	0	0	0	1	0	0
W_{13}:	0	0	0	0	0	0	0	0	0	0	0	0
W_{14}:	0	1	0	1	0	0	0	1	1	1	0	1
W_{15}:	0	1	1	0	1	0	0	0	1	1	1	0
W_{16}:	0	0	1	1	0	1	0	0	0	1	1	1
W_{17}:	0	1	0	1	1	0	1	0	0	0	1	1
W_{18}:	0	1	1	0	1	1	0	1	0	0	0	1
W_{19}:	0	1	1	1	0	1	1	0	1	0	0	0
W_{20}:	0	0	1	1	1	0	1	1	0	1	0	0
W_{21}:	0	0	0	1	1	1	0	1	1	0	1	0
W_{22}:	0	0	0	0	1	1	1	0	1	1	0	1
W_{23}:	0	1	0	0	0	1	1	1	0	1	1	0
W_{24}:	0	0	1	0	0	0	1	1	1	0	1	1

If our reception of a word is such that two errors are made, then by changing two of the characters received in all possible ways we find our original word and words differing from it in, at most, four places—the two which were wrong to start with, and the two which have been changed. But, in this way, we cannot obtain any other of the 24 words since any two differ in at least six places. With three errors the situation is different. For example, the word

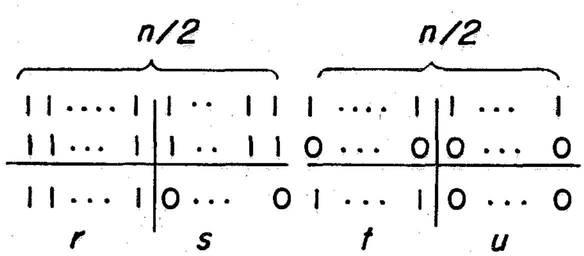
W	1	0	0	1	1	0	0	0	0	0	0	0

differs from W_{11} in three places, and from W_{12} in three other places. It also differs from W_{13} in three places. We can detect the fact that there are at least three errors, but we cannot decide with certainty which the correct word is. We say that the 24 words above form a two-error correcting, three-error detecting code.

What is the underlying algebraic theory of this code? The first twelve words are such that any two differ from each other in exactly six places. The last twelve are complements of the first twelve, obtained by interchanging zeros and ones throughout. In general, if we can find n words of length n with any two agreeing in n/2 places and disagreeing in the other n/2 places, by taking complements we will have a code of 2n words of length n. This code will correct anything less than n/4 errors and will detect errors of n/4. Thus our problem is to construct n words differing from each other in exactly n/2 places. Obviously n must be even. For n = 2 we have

$$\begin{matrix} 1 & 1 \\ 1 & 0 \end{matrix}$$

satisfying our requirements. When n is larger than 2, it turns out that n must be a multiple of 4. The number of agreements and disagreements between rows is not changed if we interchange zeros and ones in a column. Let us do this so that the first row consists entirely of ones. Then the first three rows will have a pattern of the following type:



A simple calculation shows that

$$r + s = n/2, \qquad t + u = n/2$$
$$r + t = n/2, \qquad s + u = n/2$$
$$r + u = n/2, \qquad s + t = n/2$$

comparing the rows two at a time. From this it follows that $r = s = t = u$ and so $n = 4r$ is a multiple of 4. It is conjectured that every multiple of 4 may be used to form such a code. Methods developed in 1933 by R. E. A. C. Paley gave all multiples of 4 up to 88, and many further values, but not until a few weeks ago was a code developed for the number 92 using a high speed computer at the Jet Propulsion Laboratory.

The cyclic pattern of words W_2 through W_{12} above is easily seen. It can be described by using the prime number 11 and squares of positive numbers to place the five 1's (except for column ∞) by the rules

$$1^2 = 1 \quad + 0\cdot 11$$
$$2^2 = 4 \quad + 0\cdot 11$$
$$3^2 = 9 \quad + 0\cdot 11$$
$$4^2 = 5 \quad + 1\cdot 11$$
$$5^2 = 3 \quad + 2\cdot 11$$

Thus, for W_2 we place 1's in columns ∞, 1, 3, 4, 5 and 9. In the same way, for primes 19, 23, 31, of the form $4r - 1$ we may use the same sort of rule to construct a code of 8r words of 4r dots and dashes. But to obtain 92 as a value for 4r a more complicated procedure was needed.

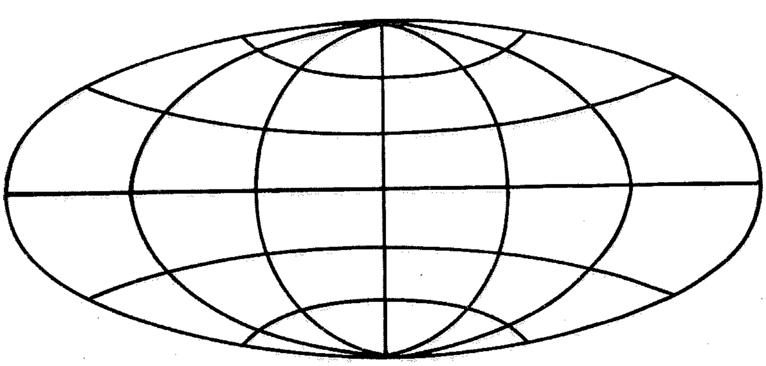
Military problems of logistics

This particular problem is a problem of arrangement and, as such, is a more sophisticated version of simple problems on permutations and combinations. Other problems of this kind which have been studied are military problems of logistics. For example, how shall we plan to send spare parts and other supplies to outer bases with the greatest expectation of satisfying all needs and yet proceeding economically? How can we schedule oil tankers to bring oil from the production centers to the centers of consumption, so as to make full deliveries with the minimum number of ships?

The assignment problem

As a final illustration of this approach I shall mention the assignment problem. This is the problem of assigning n men to n jobs, when we are given rating scores a_{ij}, i, j running from 1 to n as to the value of the ith man in the jth position, so as to make the sum of the scores for the selection as large as possible. These scores may be the result of competitive tests, or may be a summary of the opinions of superiors. The source of the scores is not our concern here, and for our purposes they can be any random assortment of positive integers. Here is a table of scores for 8 men and 8 positions:

continued on page 24



Positions

Men	1	2	3	4	5	6	7	8
1	1	5	4	7	7	3	6	6
2	4	2	5	4	6	1	2	5
3	6	5	2	4	4	2	5	3
4	7	1	7	3	3	2	1	5
5	3	6	7	3	2	5	5	4
6	7	5	6	7	6	1	4	6
7	6	1	5	2	2	1	7	3
8	4	4	7	3	2	1	3	1

The method consists in using row numbers $r_1, \ldots, r_n$ and column numbers $c_1, \ldots, c_n$, such that in every case $a_{ij} \leq r_i + c_j$. This can certainly be done by taking all row numbers to be zero and taking c_j to be the largest value in the jth column. For any selection of n scores – one from each row and column – we certainly have $a_{1s} \leq r_1 + c_s \ldots, a_{nz} \leq r_n + c_z$. Hence $a_{1s} + \cdots + a_{nz} \leq r_1 + \cdots + r_n + c_1 + \cdots + c_n$ since every column is used exactly once. Thus our maximum selection score cannot possibly be greater than the sum $S = r_1 + \cdots + r_n + c_1 + \cdots + c_n$ for any choice of row and column numbers such that $r_i + c_j \geq a_{ij}$ for all i and j. It can be shown that if we cannot make a selection from those top scores a_{ij} which are big enough so that $a_{ij} = r_i + c_j$ then it is possible to increase some of the r's and c's and decrease others in such a way as to reduce the sum S. When S can no longer be reduced it will be possible to make a selection in at least one way so that S is the maximum score possible for an assignment.

In our case, we originally take all row numbers 0, and column numbers 7, 6, 7, 7, 7, 5, 7, 6, with $S = 52$ thus:

Positions

Men	1	2	3	4	5	6	7	8	ri
1	1	5	4	7	7	3	6	6	0
2	4	2	5	4	6	1	2	5	0
3	6	5	2	4	4	2	5	3	0
4	7	1	7	3	2	5	5	4	0
5	3	6	7	3	2	5	5	4	0
6	7	5	6	7	6	1	4	6	0
7	6	1	5	2	2	1	7	3	0
8	4	4	7	3	2	1	3	1	0
cj	7	6	7	7	7	5	7	6	

We find there are no top scores in the second or third row and so a selection from these top scores is not possible. Having failed in our first attempt, let us reduce all column numbers by 1 and replace the row numbers by 1, 0, 0, 1, 1, 1, 1, 1. We have decreased our column total by 8. S is now reduced to 50 and the condition $r_i + c_j \geq a_{ij}$ still holds in all cases. Let us circle the top scores for this choice:

Positions

Men	1	2	3	4	5	6	7	8	
1	1	5	4	7	7	3	6	6	1
2	4	2	5	4	6	1	2	5	0
3	6	5	2	4	4	2	5	3	0
4	7	1	7	3	3	2	1	5	1
5	3	6	7	3	2	5	5	4	1
6	7	5	6	7	6	1	4	6	1
7	6	1	5	2	2	1	7	3	1
8	4	4	7	3	2	1	3	1	1
	6	5	6	6	6	4	6	5	

The optimal assignments

We can now find an assignment from these top scores. There are in fact three different ways of doing this:

Men	1	2	3	4	5	6	7	8
Position Assignment	4	5	2	1	6	8	7	3
	8	5	2	1	6	4	7	3
	5	8	2	1	6	4	7	3

Assignment score S = 50.

Notice that in all three assignments we must place the third man in the second position, even though this is not the best score possible for the man or the best score possible for the position.

A set of rules is known so that whenever a particular set of row and column numbers, such as our first choice, does not give an assignment from the top scores, then the row and column numbers can be altered to give a smaller value for S. This process can be continued until an assignment can be found from top scores giving us the value of S as the assignment score. In our example we reached this stage in our second choice of row and column numbers.

Algebra – holding its own

In summary, algebra is doing better than holding its own in modern technology. There seems to be no end to the sequence of new and difficult problems which keep arising, but successful solutions are numerous and encouraging for the future.