HADAMARD MATRICES

George Szekeres

Suppose that n players are engaged in a round robin tennis tournament, that is each player plays each of the other $n-1$ players exactly once. Suppose also that the number of players is even, $n = 2m$. Can the outcome of the tournament be such that if you take any two of the players, A and B say, then among the other $2m-2$ players there are exactly $m-1$ (that is exactly half of them) against whom A and B score the same result, that is either both win or both lose (there are no draws in tennis). For instance if there are four players, the following scores table will have the required property.

	A	B	C	D
A	0	+	+	+
B	−	0	−	+
C	−	+	0	−
D	−	−	+	0

In the table + stands for a win, − stands for a loss. No player plays of course against himself, hence the 0 in the "diagonal" positions. For example A and B both win against D, or B and C both lose against A, and similarly for the other four pairs. In the case of six players you will find after some experimenting that it is impossible to find a score table which would satisfy the condition, and if you are sufficiently persistent, you may be able to come up with a table for eight players.

Looking at such a problem superficially you may be inclined to think that this is just one of those tricky competition problems that a bright student might easily be able to solve. In point of fact it is a very difficult question which has puzzled mathematicians for well over 100 years and a complete answer seems as elusive as ever.

If you think of the symbols + and − in the score table as +1 and −1, we have a matrix of order n, the technical name for a double array of numbers with n "rows" and n "columns". Our condition is that if we take any two rows in the matrix and compare entries in the same position (that is belonging to the same column), the total number of (++) and (−−) pairs should be the same as the total number of (+−) and (−+) pairs.

Denote by a_{ij} the matrix entry in the i-th row and j-th column (so that for $i \neq j$, a_{ij} is either $+1$ or -1 and $a_{ii} = 0$ for all i). Perhaps you have noticed already that $a_{ji} = -a_{ij}$ for all i, j since if A wins against B then B loses against A.

A little thought will convince you that the condition we want to fulfil is this: for any pair i, j

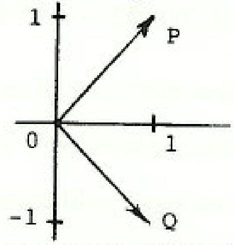
$$a_{i1}a_{j1} + a_{i2}a_{j2} + \cdots + a_{in}a_{jn} = 0.$$

Using conventional mathematical symbolism, we want the equation

$$\sum_{k=1}^{n} a_{ik}a_{jk} = 0 \qquad (1)$$

to hold for all i, j, $1 \leq i < j \in n$.

For the mathematician this equation has a familiar meaning which some of you will no doubt recognise. If the entries $(a_{i1}, a_{i2}, \cdots, a_{in})$ of the i-th row are regarded as coordinates of a "vector" in an n-dimensional space then condition (1) expresses the fact that the vector formed by the i-th row of the matrix is "perpendicular" or "orthogonal" (these two things mean the same) to all vectors formed by the other rows. (Their "scalar product" is 0; see for this terminology the article by Brian Jefferies in an earlier issue of **Parabola**.) Take for instance in the plane ($n = 2$) the vectors from (0,0) to the points $P = (1,1), Q = (1,-1)$, as shown in the figure.



Since $1 \times 1 + 1 \times (-1) = 0$, equation (1) is satisfied, and indeed the two vectors are perpendicular to each other in the ordinary sense, as you can see by simple geometry.

Let us modify slightly our original problem of tournaments. For what values of n is it possible to construct a matrix of order n with all entries $+1$ or -1 such that all pairs of rows should satisfy equation (1)? Notice that we don't put 0's in the diagonal of the matrix and also we don't necessarily require the "tournament condition" $a_{ji} = -a_{ij}$. In this form the problem was first posed by the famous British mathematician Sylvester some 125 years ago. The true importance of the problem was recognised 25 years later by the French mathematician Hadamard (one of the great figures of turn-of-century mathematics) and later workers on the problem named ± 1 matrices with mutually orthogonal rows after Hadamard.

It is clear that Hadamard matrices (H-matrices for short) can only exist for even n, since all product terms in (1) are $+1$ or -1 and the sum of an odd number of $\pm$ 1's can never be 0. Not quite so obvious is the fact that n must be divisible by 4 (except when $n = 2$ for which an H-matrix obviously exists). I leave the verification of this as a problem for you to think about. Sylvester suggested that perhaps an H-matrix exists for all orders n which are divisible by 4. (He of course did not speak of Hadamard matrices; Hadamard was barely 2 years old when Sylvester stated his problem). At any rate Sylvester only demonstrated that if an H-matrix of order n exists then also one of order $2n$ exists. The proof is quite simple. If A stands for an H-matrix of order n, take the following matrix of order $2n$: $\begin{pmatrix} A & A \\ A & -A \end{pmatrix}$, that is, place A in the upper left hand corner, another copy of A in the upper right hand and lower left hand corners, and $-A$ in the lower right hand corner. Here $-A$ denotes the matrix obtained from A by changing the sign of each entry, that is change every $+1$ into -1 and every -1 into $+1$. For instance $\begin{pmatrix} + & + \\ + & - \end{pmatrix}$ is obviously an H-matrix of order 2 and therefore Sylvester's duplication construction yields an H-matrix of order 4, namely $\begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}$.

Repeating the construction we can obtain an H-matrix of orders 8, 16, $32, \cdots, 2^k$ for all k.

It follows generally that if an H-matrix of order n exists then also one of order $2^k n$ exists for $k = 0, 1, 2, \cdots$. Therefore to show the truth of Sylvester's conjecture it would be quite sufficient to produce an H-matrix for all orders $4m$ where m is an odd number. At present no general method is known which would supply an H-matrix of order $4m$ for all odd m except for certain special values of m. Hadamard himself gave an example of an H-matrix of order 12, and Paley showed in 1933 that there exists an H-matrix of order $4m$ whenever $4m - 1$ is a prime number.

I shall explain Paley's ingenious construction, although some details will have to be omitted. First a few words about Paley himself. He was one of the most gifted young mathematicians of the early thirties in Cambridge. He also loved mountain climbing and skiing, and in 1933 (the year he wrote his paper on H-matrices), while on a holiday in the Canadian Rockies, he crashed to his death in an avalanche at the age of 26. In his four mathematically active years (from 1930 to 1933) he wrote about 30 mathematical papers, most of them of permanent value. G.H. Hardy, the leading British mathematician of his time, wrote in his obituary of Paley that the young research student was so incredibly quick in absorbing difficult mathematical ideas that he almost frightened Hardy by his sheer brilliance.

Here is the essence of Paley's construction. Let p be a prime number of the form $4m-1$, such as 3,7,11,19 etc. Suppose $F(a)$ is a function defined for all integers a (positive or negative) with the following properties:

(i) $F(0)=0,\ F(1)=1,\ F(-1)=-1$

(ii) $F(a)=+1$ or -1 for all integers a between 1 and $p-1$

(iii) $F(a+p)=F(a)$ for all integers a

(iv) $F(a,b)=F(a),F(b)$ for all integers a,b.

Such a function is well known to mathematicians, under the name of "Legendre's symbol", after the 18-th century French mathematician Legendre who first defined this function for number theoretical purposes. How does one construct Legendre's function? Property (iii) tells us that F has "period" p, that is

$$F(a)=F(a+p)=F(a-p)=F(a+2p)=F(a-2p)=\cdots \text{ etc.}$$

For instance $F(p-1)=F(-1)=-1,\ F(p)=F(0)=1$ by property (i). Therefore it is quite sufficient to define $F(a)$ for $a=1,2,\cdots,p$. (We can always add or subtract from a a suitable multiple of p so that $a+kp$ or $a-kp$ should fall between 1 and p). For instance $F(a)=0$ for every a which is divisible by p and is $+1$ or -1 for all other values of a. The "difficult" property to satisfy is the last one, namely $F(a,b)=F(a).F(b)$. There is nothing to worry about when either a or b is divisible by p since then both sides of the equation are 0. But what about those values of a and b which are not divisible by p? To demonstrate how it is done, I shall confine the discussion to the case of $p=11$.

Define $F(2) = -1$ and generally $F(2^k) = (-1)^k$ for $k = 0, 1, 2, \cdots$. This is certainly a sneaky way to satisfy property (iv) since

$$F(2^i.2^j) = F(2^{i+j}) = (-1)^{i+j} = (-1)^i.(-1)^j = F(2^i).F(2^j).$$

So condition (iv) is satisfied at least for the numbers of the form $a = 2^k$. But don't we eventually get into conflict with condition (iii)? And even if there is no conflict, is $F(a)$ then defined for all a? Let us first verify that we do get a value for $F(a)$ when $a = 1, 2, \cdots, 10$. (Remember: p is now 11). From the first four values $k = 0, 1, 2, 3$ we get $F(2^0) = F(1) = (-1)^0 = 1$ (as it should be, according to (i)), $F(2^1) = F(2) = (-1)^1 = -1$, $F(2^2) = F(4) = (-1)^2 = 1$, $F(2^3) = F(8) = -1$, so we have defined $F(a)$ for $a = 1, 2, 4, 8$. Next $F(2^4) = F(16) = F(16-11) = F(5) = (-1)^4 = 1$ (we assume here property (iii)) and similarly $F(2^5) = F(32) = F(10) = -1$ (as it should be, according to (i)), namely $F(10) = F(-1) = -1$), $F(2^6) = F(64) = F(9) = 1$), $F(2^7) = F(128) = F(7) = -1$, $F(2^8) = F(256) = F(3) = 1$, $F(2^9) = F(512) = F(6) = -1$. We have now the complete set of values of $F(a)$ for $a = 1, 2, \cdots, 10$, namely

a	1	2	3	4	5	6	7	8	9	10
$F(a)$	1	-1	1	1	1	-1	-1	-1	1	-1

Admittedly, a crazy looking collection of values, but there is method in the madness. The values were obtained by a perfectly orderly prescription, namely by taking the values of $F(2^k)$ for $k = 0, 1, 2, \cdots, 9$ and using property (iii) to pull 2^k down to the interval [1,10].

What about if we continue past $k = 9$ and apply property (iii), don't we get into conflict? Take for instance $k = 10$. We get $F(2^{10}) = F(1024) = F(1 + 93 \times 11) = F(1) = 1$, as it should be since $(-1)^{10} = 1$. Those of you who have heard about Fermat's theorem will know that not only for 11 but for any prime number $p > 2$ it is true that $2^{p-1} - 1$ is divisible by p, hence $F(2^{p-1}) = F(1) = 1 = (-1)^{p-1}$, as it should be. More generally $2^{k+p-1} - 2^k = 2^k(2^{p-1} - 1)$ is divisible by p and so $F(2^{k+p-1}) = F(2^k) = (-1)^k = (-1)^{k+p-1}$ (since $p - 1$ is even) and there is no conflict with property (iii). We have obtained a perfectly valid definition of $F(a)$ for all a, at least when $p = 11$.

At this stage you may wonder why have I carried out the construction for $p = 11$ and not for say 7 which surely would have taken less time and effort. There is a little snag with $p = 7$ (two snags, to be precise). Suppose you define, as before, $F(1) = 1$, $F(2) = -1$, $F(4) = 1$. What about $F(2^2) = F(8)$? This ought to be $(-1)^3 = -1$, but also $F(8) = F(8-7) = F(1) = 1$, and we get into contradiction. There is another trouble here, not unrelated to the first one: $F(3)$ cannot be obtained in this way because there is no power of 2 which would give remainder 3 when divided by 7, that is $2^k - 3$ is not divisible by 7 for any k (prove it). Both troubles are avoided if we define $F(a)$ not through powers of 2 but powers of 3: $F(1) = 1$, $F(3) = -1$, $F(3^2) = F(9) = F(2) = 1$, $F(3^3) = F(27) = F(6) = -1$, $F(3^4) = F(81) = F(4) = 1$, $F(3^5) = F(243) = F(5) = -1$, and everything is fine. We now have the table:

a	1	2	3	4	5	6
$F(a)$	1	1	-1	1	-1	-1

Note that $F(-1) = F(6) = -1$, as required by property (i). For an arbitrary prime number of the form $4m - 1$ we need to find a suitable "base" b (instead of 2) which has the property that $b^0, b^1, b^2, \cdots, b^{p-2}$ provide all the remainders $1, 2, \cdots, p-1$ (in some wild order) when divided by p. Such a base always exists, but a proof is beyond the scope of this article. It was the young Gauss who first gave a full proof of this fact, although it was known to Euler 50 years earlier.

Now back to Paley's construction. He defines the entries of his H-matrix of order $n = 4m = p + 1$ by the formula

$$a_{ij} = F(i - j) \text{ for } i \le i \le p,\ 1 \le j \le p,\ i \ne j$$

$$a_{in} = 1,\ a_{ni} = -1 \text{ for } 1 \le i \le p = n - 1$$

$$a_{ii} = 1 \text{ for } 1 \le i \le n = p + 1.$$

With this definition the orthogonality equations (1) are indeed satisfied but by now I am sure I have exhausted the patience of the reader and don't give the proof. It requires a slightly tricky calculation, using all the properties (i) - (iv) of F. I only mention that

$$a_{ji} = F(j - i) = F((-1).(i - j)) = F(-1).F(i - j) = -a_{ij}$$

hence Paley's H-matrix satisfies the tournament condition too. In fact if you replace the diagonal entries $a_{ii} = 1$ by $a_{ii} = 0$, you get a solution for my original tournament problem, at least for those $n = 4m$ which are of the form $p = 1$, p prime.

To finish off let me illustrate Paley's construction by an example. Take $n = 8 = 7 + 1$ for which we have already found the values $F(a)$ earlier. Then $a_{21} = F(2-1) = F(1) = 1$, $a_{31} = F(3-1) = F(2) = 1$, $a_{41} = F(4-1) = F(3) = -1$ and so on, and we obtain the following H-matrix of order 8:

$$\begin{array}{cccccccc}
+ & - & - & + & - & + & + & + \\
+ & + & - & - & + & - & + & + \\
+ & + & + & - & - & + & - & + \\
- & + & + & + & - & - & + & + \\
+ & - & + & + & + & - & - & + \\
- & + & - & + & + & + & - & + \\
- & - & + & - & + & + & + & + \\
- & - & - & - & - & - & - & +
\end{array}$$

Problems.

1. If A is an H-matrix, show that interchanging two columns of A or multiplying the entries in a column by -1 will yield another H-matrix.
2. Using this fact or otherwise, show that the order of an H-matrix must be divisible by 4, except when $n = 2$.
3. Show that Sylvester's duplication construction does give an H-matrix.
4. Suppose that A is an H-matrix with the additional "tournament" property $a_{ji} = -a_{ij}$ for all $i \neq j$ and $a_{ii} = 1$ for $i = 1, 2, \cdots, n$. Find a duplication construction which results in an H-matrix of order $2n$ which still satisfies $a_{ji} = -a_{ij}$ for all $i \neq j$.
5. Following Paley's method construct an H-matrix of order 12.
6. Prove that there are infinitely many prime numbers of the form $4m-1$. Hint: (for those who are familiar with Euclid's proof that there are infinitely many prime numbers). Suppose that there are only a finite number of such primes, $p_1, p_2, \cdots p_n$ say. Prove that (i) for each p_i, p_i^2 is of the form $4k + 1$, (ii) the number

$$P = p_1^2 p_2^2 \cdots p_n^2 - 2$$

is of the form $4k - 1$, (iii) P has a prime divisor of the form $4k - 1$, distinct from all the p_i.