Parabola Volume 41, Issue 3 (2005)

Unsolved Problems 2[1]

George Szekeres

The theory of combinatorial configurations abounds in unsolved problems, some of which can be stated in simple non-technical terms. One of the most famous among these is the following problem due to the French mathematician, J. Hadamard.

Given an odd number of the form $n = 4m - 1$, is it possible to select from among the subsets of the set of numbers $\{1, 2, \dots, n\},\ n$ subsets $S_1, S_2, \dots, S_n$ such that

(i) each S_i contains exactly $2m - 1$ numbers, and

(ii) every pair of subsets $S_1, S_j\ (i \neq j)$ has exactly $m - 1$ numbers in common?

Hadamard formulated his problem slightly more technically, in terms of so-called orthogonal matrices, but it can easily be shown to be equivalent to the combinatorial problem stated above.

Hadamard configurations (or briefly, H. configurations) are known to exist for many values of m, and Hadamard conjectured that they exist for every m, but no one has yet been able to supply a general proof. A number of new H. configurations have recently been discovered with the help of fast electronic computers. At present, the lowest value of m for which no one has yet been able to produce an H. configuration is $m = 29$.

For small values of m a little experimenting will readily yield H. configurations. In the case of $m = 1,\ n = 3$, we have the trivial configuration

$$S_1 = (1),\ S_2 = (2),\ S_3 = (3).$$

In the case of $m = 2$ we are required to find 7 subsets containing 3 elements each so that every pair will have exactly one element in common.

$$\begin{aligned} &S_1 = (123), \quad S_2 = (145), \quad S_3 = (167), \\ &S_4 = (246), \quad S_5 = (257), \quad S_6 = (347), \quad S_7 = (356) \end{aligned}$$

is such a configuration.

It is easy to show that if there exists an H. configuration for $n = 4m - 1$ then there also exists one for $2n+1 = 8m-1$. If S is a subset of $M = \{1, 2, \dots, n\}$, let us denote by S' the complement of S in M, that is the subset of those elements of M which are not in S. For example, if $n = 7$ and $S = (145)$ then $S' = (2367)$. Clearly if S contains $2m - 1$ elements then S' contains $n - (2m - 1) = 2m$ elements.

Denote now by S'' the subset of $N = (1, 2, \dots, n,\ n+1, \dots, 2n+1)$ obtained from S by adding n to each of its elements. For example, in the previous case when $S = (145)$, we have $S'' = (8, 11, 12)$. The reader should verify that

[1] This article is reprinted from *Parabola* Vol. 2, No.3, 1965.

(a) If S_1 and S_2 are subsets of M, each containing $2m-1$ elements and having $m-1$ elements in common then S_1 and S_2' have m elements in common.

(b) If $S_1, \ldots, S_n$ is an H. configuration of M then the following $2n+1$ subsets of n form an H. configuration:

$$\begin{array}{ll} (S_i, S_i'',\ 2n+1), & i = 1, 2, \ldots, n \\ (S_i, S_i''), & i = 1, 2, \ldots, n \\ M'' = n+1, \ldots, 2n. & \end{array}$$

From (b) it follows that there exists an H. configuration for every $m = 2^k,\ k = 0, 1, 2, \ldots$. The first value of m not of this form is $m = 3$.

The reader should try to construct a Hadamard Configuration for $m = 3,\ n = 11$.

Commentary by Catherine Greenhill

In this article George Szekeres described the Hadamard problem, which he described as one of the most famous unsolved problems. It is due to the French mathematician, Jacques Hadamard (1865 – 1963).

Given an odd number of the form $n = 4m - 1$, can you find subsets $S_1, \ldots, S_n$ of the set $\{1, \ldots, n\}$ such that each S_i contains $2m-1$ elements, and if $i \neq j$ then S_i and S_j have exactly $m-1$ elements in common?

George called such a set of subsets a Hadamard configuration, or H-configuration for short. Today, we call them Hadamard designs. Hadamard conjectured that H-configurations exist for all $m \geq 1$. Various different constructions are known. In his article, George described how to construct an H-configuration for $n = 8m-1$, assuming that you know one for $n = 4m-1$. He also mentioned that "fast electronic computers" were helping for the search for H-configurations, and that in 1965 the lowest value of m for which no H-configuration was known was $m = 29$.

Hadamard's conjecture is still unsolved, and it is still one of the most important open problems in combinatorics. A H-configuration (or Hadamard design) with $n = 4m-1$ corresponds to Hadamard matrices of size $4m \times 4m$. Hadamard matrices are also objects of great interest which are used in the design of error-correcting codes.

Meanwhile, our fast, electronic computers have indeed been very helpful in the search for H-configurations. In 1985 Sawade found a H-configuration with $m = 87$, then for a long while $m = 107$ was the smallest value for which there was no known H-configuration. A very recent development was the discovery in 2004 of a H-configuration with $m = 107$. So now the smallest value of m for which no H-configuration is known is $m = 187$.