the acceptance of a falsely corrected input. If this is disastrous, the double digit should be used without correction. Otherwise it may be satisfactory simply to list the automatic corrections made for subsequent checking. The check digits increase the punching by between $2\frac{1}{2}$ per cent on an 80-column card and $33\frac{1}{3}$ per cent on the key alone, but this is outweighed by the possibility of omitting card verification.

Yours faithfully,
Dr. K. M. Howell

Management Services Department
ICI Fibres
Hookstone Road
Harrogate
Yorkshire HG2 8QN
29 November 1974

To the Editor
The Computer Journal

Sir

Your correspondent, A. M. Andrew seeks a method of detecting and correcting errors in a two digit number using a further two digits only. I believe one solution to be the following.

Let the message to be transmitted be *mnab* where m and n are any two digits and a and b are given by:

$$a = |n + m|_{10}$$
$$b = |n - m|_{10} \; .$$

If the received message is *MNAB* then we form the following differences:

$$d_1 = |A - (N + M)|_{10}$$
$$d_2 = |B - (N - M)|_{10} \; .$$

The original message is reconstructed as follows.

If $d_1 = d_2 = 0$ then $m = M$, $n = N$, $a = A$, $b = B$

If $d_1 = d_2 \neq 0$ then $m = M$, $n = |N + d_1|_{10}$, $a = A$, $b = B$

If $d_1 = |-d_2|_{10}$ then $m = |M + d_1|_{10}$, $n = N$, $a = A$, $b = B$

If $d_1 = 0$ and $d_2 \neq 0$ then $m = M$, $n = N$, $a = A$, $b = |N - M|_{10}$

If $d_1 \neq 0$ and $d_2 = 0$ then $m = N$, $n = N$, $a = |N + M|_{10}$, $b = B$

If $d_1 \neq |\pm d_2|_{10}$ then more than one error has occurred.

Yours faithfully,
B. M. Ewen-Smith

5 Finch's Field
Little Eversden
Cambridge
1 December 1974

To the Editor
The Computer Journal

Sir

Decimal error-correction—a solution

In my letter which you were kind enought to publish in your issue for November 1974, I referred to the problem of assigning two check digits to a two-place decimal number so as to achieve correction of single errors. I did not then realise that the problem is equivalent to that of forming a Graeco-Latin square of order ten.

A Latin square of order n is a square array containing n symbols, with each symbol occurring once in each row and once in each column. A Graeco-Latin square is a superposition of two Latin squares, traditionally using symbols from the Latin alphabet for one and from the Greek alphabet for the other. The two Latin squares must be orthogonal in that there are no two cells holding the same pair of symbols; a Latin symbol is paired with a different Greek symbol in each of its n occurrences and *vice versa*. **Table 1** shows a Graeco-Latin square of order ten, in which the digits 0-9 are used instead of Latin and Greek letters. The required error-correcting code is achieved simply by letting the two message digits select a row and column and using the two digits in the selected cell as check digits. The four-digit messages then have Hamming distance three, and single-error correction is possible.

Latin squares are treated very fully by Denes and Keedwell (1974). Prior to 1959 it was generally thought there were no Graeco-Latin squares of order ten; Euler had conjectured there were none for any order expressible as $4n + 2$. Parker (1959) published the first Graeco-Latin square of order ten, and Table 1 represents a re-labelling of the form given by Fisher and Yates (1963), which is a rearrangement of Parker's original.

It is also known that Graeco-Latin squares exist for all powers greater than ten expressible as $4n + 2$, but as shown by Fisher and Yates (1934) there is none of order six. It is easily shown that the existence of a Graeco-Latin square is a necessary as well as a sufficient condition for error-correction with two message and two check digits, so Golay's doubts about the possibility of error-correction with radix six are fully justified. Golay (1958) was considering five message and two check digits, but if correction is impossible for two message digits it is also impossible for any greater number.

Mann (1943) has given a method for constructing Latin squares which produces two or more orthogonal squares, as required to form a Graeco-Latin square, except where the order is expressible as $4n + 2$. With the later findings of Parker and of Bose and Shrikhande (1959) on squares whose order is expressible in that form, it appears that error-correction with two message and two check digits is possible for any radix except two and six. For either of these it is impossible.

Yours faithfully,
A. M. Andrew

References

Bose, R. C., and Shrikhande, S. S. (1959). On the falsity of

Table 1 Graeco-Latin square

	0		1		2		3		4		5		6		7		8		9	
0	0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9
1	1	2	2	0	0	1	6	8	7	9	8	3	9	4	3	5	4	6	5	7
2	2	1	0	2	1	0	5	4	6	5	7	6	8	7	9	8	3	9	4	3
3	3	7	7	3	8	9	0	6	1	8	4	0	2	5	5	2	9	1	6	4
4	4	8	8	4	9	3	7	5	0	7	1	9	5	0	2	6	6	2	3	1
5	5	9	9	5	3	4	4	1	8	6	0	8	1	3	6	0	2	7	7	2
6	6	3	3	6	4	5	8	2	5	1	9	7	0	9	1	4	7	0	2	8
7	7	4	4	7	5	6	2	9	9	2	6	1	3	8	0	3	1	5	8	0
8	8	5	5	8	6	7	9	0	2	3	3	2	7	1	4	9	0	4	1	6
9	9	6	6	9	7	8	1	7	3	0	2	4	4	2	8	1	5	3	0	5